WiMAX Forum® System Profile Requirements for Smart Grid Applications

Requirements for WiGRID

WMF-T31-002-R010v01

WMF Approved

(2013-02-05)

WiMAX Forum Proprietary

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability

Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance of the following terms and conditions:

THIS DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY.

Any products or services provided using technology described in or implemented in connection with this document may be subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable jurisdiction.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.

The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, technologies, standards, and specifications, including through the payment of any required license fees.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT.

IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS MEMBERS RELATING TO THE USE OF THIS DOCUMENT.

The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is solely responsible for determining whether this document has been superseded by a later version or a different document.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1. Introduction and Document Objective

1.1 General Information

Electric utilities require nearly ubiquitous telecommunications coverage over their service areas to enable "Smart Grid" functionality. Smart Grid functionality relies on the availability of a reliable communications medium to reach the following:

- Power line and transformer sensors for wide area situational awareness – for telemetry. These low power devices may include sensing functionality such as fault indication, voltage, current, line vibration, line temperature, and metering.
- Smart meter collection points (AKA Data Aggregation Points, DAPs) – for backhaul of IEEE 802.15.4g [5] based, Smart Utility Network, Mesh Neighborhood Area Networks.
- Pole mounted Distribution Automation Equipment – for protection, control and monitoring. These devices may require Layer 2 for GOOSE status messages, or other similar protocols
- Distributed Generation (renewable energy) – for protection, control, and monitoring. This emerging class of generation requires greater control and monitoring of the distribution system. This is in part due to the wide geographic distribution, point of interconnection (on primary or secondary distribution system), and variability of the generation sources (e.g. solar, wind, and PEV).
- Power generation plants and substations – for protection, control, monitoring and workforce. These locations are typically in remote areas outside of reach of conventional telecommunications offerings.

Wireless technology may provide cost effective coverage, complementary to wireline. For most SG applications, high availability and reliability is essential. The following are common characteristics;

Reliability;

- Regardless of the environment, society expects electricity to be available.
- Asset management requires the ability to monitor, control, and forecast the usage.
- The communications network needs to be stable, predictable and robust.

Security;

- The network must be secure and trustworthy. Trustworthy means the information has not been modified, deleted or added to by an unauthorized party.
- No network disruption.
- High level of privacy is essential to prevent unauthorized and malicious use of personal and other information being transmitted on the network.

Integration and support of the existing infrastructure.

- Utilities have a variety of different legacy technologies which continue to be reliable.
- Upgrades and changes have to be evolutionary not revolutionary

Support of smart metering.

- Enable more efficient use of energy resources.
- Mainly fixed and nomadic modes of operation.

- The majority of the information is from the distribution, so UL biased. Exceptions will occur during system-wide firmware downloads.

Corrective action needs to be fast to minimize any shutdown.

- Low and predictable latency.
- Systems need to work when cutoff from the main network.

Utilities often have personnel working at permanent and or temporary remote sites, for instance;

- The maintenance of transmission lines and generation facilities.
- The construction of transmission lines and generation facilities.
- The repair of transmission and generation facilities.

These activities either require communications or are made more efficient by using communications by means of verifying or diagnosing faults, commissioning systems and providing workforce communications.

1.2 General Aspects of Throughput and Latency

The capacity (Goodput) and latency requirements specified by the OpenSG-Net working group and PAP2 are based on performance requirements at the ‘Application Layer’ WiMAX/WiGRID simulation methodology mirrors IMT-Advanced (4G) in which spectral efficiency (or throughput) is specified as “IP layer output” to “IP layer input” as shown on the following diagram. Latency is defined similarly. This, of course, differs from the metrics that OpenSG-Net specifies, which is Actor A to Actor B as shown in the diagram. In the comparison of alternative technologies the OpenSG assumption for higher layer overhead is about 20%. So far no conclusions have been arrived for estimates of higher layer latency.

Notes:

- VoIP traffic will not be a dominant service for SG
- Some SG use cases have latency-sensitive data traffic. This will want a mechanism to “Tag” selected SG data packets as UGS or ertPS to give them priority to meet latency requirements.

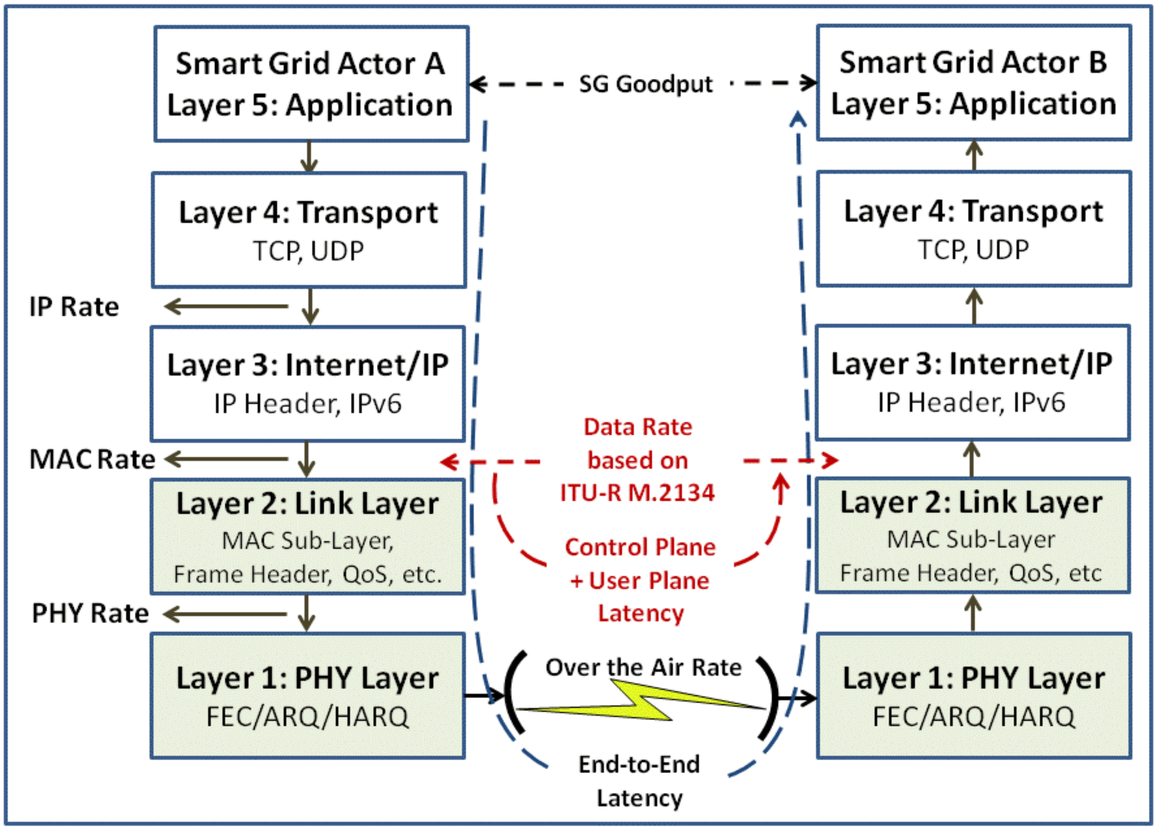


Figure 1 – Protocol layers

1.3 Latency Budget

Power utilities have latency and service flow requirements based on the type of application being addressed. The application and typical associated service flows are tabulated below;

Application	Service flow type
Smart metering	Best Effort
Distribution automation	Unsolicited Grant Service
SCADA	Non Real Time Polling Service

Of the above applications, distribution automation in terms of latency is the most difficult to achieve. With reference to IEC 61850-5[1] the latency of the communication system is part of what is defined as the transfer time for the complete transmission of a message from one automation device to another. The figure below derived from IEC 61850 shows the message being sent from device f1 to device f2 and the communications network between the two devices. The breakdown of the transfer time components is shown for the different parts of the communications system;

[1] IEC 61850-5, Communication networks and systems in substations – Part 5: Communication requirements for functions and device models

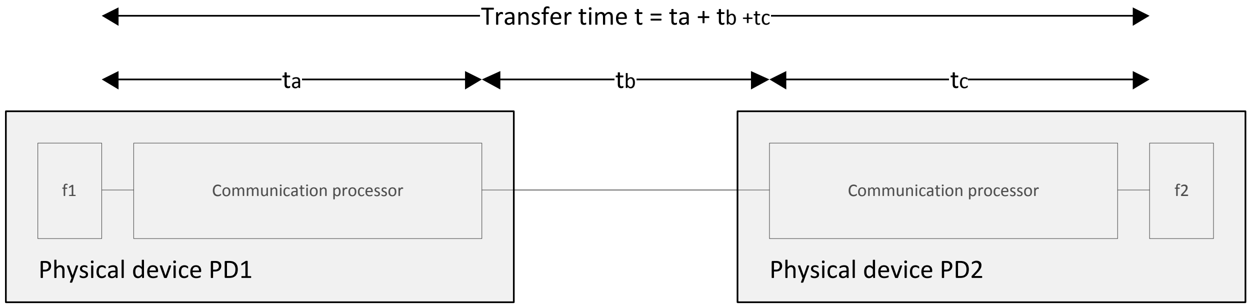


Figure 2 – Latency baseline

From this, the communications path could either be from WiMAX® CPE to WiMAX base station, (or vice versa);

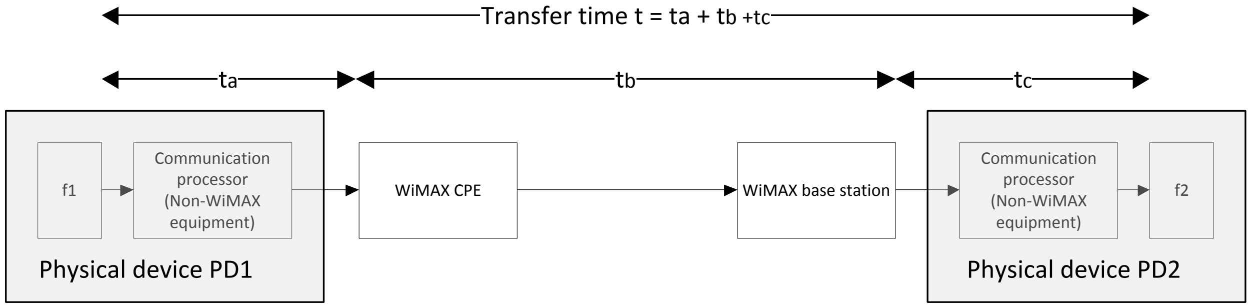

Transfer time t = ta + tb +tc
ta
tb
tc
f1
Communication processor (Non-WiMAX equipment)
WiMAX CPE
WiMAX base station
Communication processor (Non-WiMAX equipment)
f2
Physical device PD1
Physical device PD2

Figure 3 – WiMAX CPE to base station

Or from WiMAX CPE via a base station to another WiMAX CPE, this assumes local switching of traffic at the base station as opposed to the traffic traversing a core network.

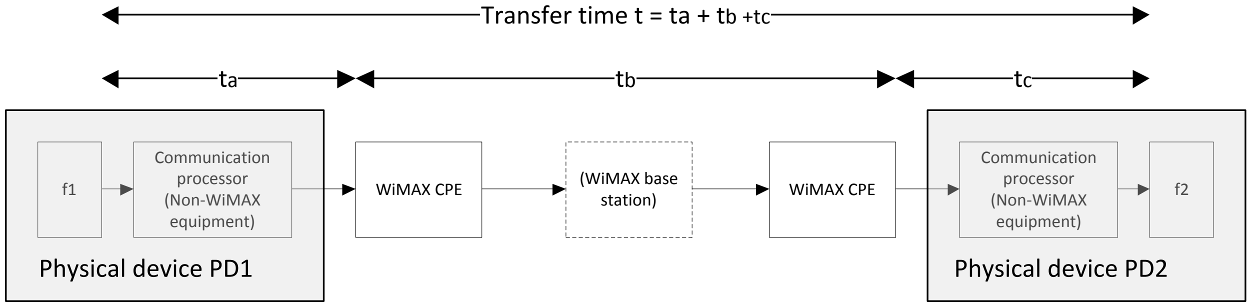

Transfer time t = ta + tb +tc
ta
tb
tc
f1
Communication processor (Non-WiMAX equipment)
WiMAX CPE
(WiMAX base station)
WiMAX CPE
Communication processor (Non-WiMAX equipment)
f2
Physical device PD1
Physical device PD2

Figure 4 – WiMAX CPE to CPE via base station with local switching

Noting that there are scenarios where the WiMAX CPE for f1 may not be connected to the same base station as the WiMAX CPE for f2 as below;

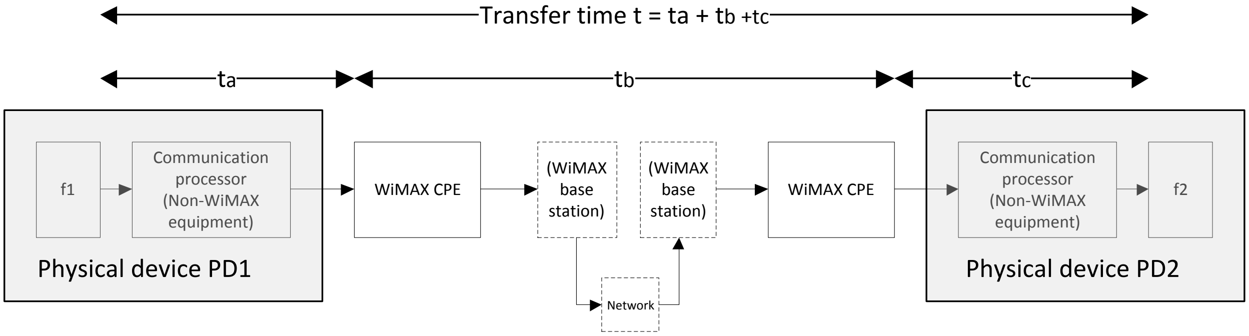

Transfer time t = ta + tb +tc
ta
tb
tc
f1
Communication processor (Non-WiMAX equipment)
Physical device PD1
WiMAX CPE
(WiMAX base station)
Network
(WiMAX base station)
WiMAX CPE
Communication processor (Non-WiMAX equipment)
f2
Physical device PD2

Figure 5 – WiMAX CPE to CPE via base station and core network

Other scenarios have all or either of the CPEs having a best and alternate base station sector for increased reliability; this could imply that the transfer time is not the same all the time.

The communication processor within the physical device in many typical situations could have a non-WiMAX device, for the most part in these situations it is optimized to have a latency of less than 200 µs for IEC 61850 traffic. Therefore the majority of the transfer time is accounted for in the WiMAX system.

From IEC 61850 a number of message types and the transfer times are defined;

Table 1: IEC 61850 message types

IEC 61850 Message Type	Transfer Time	Transportable by WiMAX based on 5 ms frame
Type 1, Fast messages, Type 1A, Trip messages, performance class P1	In the order of 10 ms	Unlikely
Type 1, Fast messages, Type 1A, Trip messages, performance class P2 and P3	In the order of 3 ms	No
Type 1, Fast messages, Type 1B, Other messages, performance class P1	Less than or equal to 100 ms	Yes
Type 1, Fast messages, Type 1B, Other messages, performance class P2 and P3	In the order of 20 ms	Possible
Type 2, Medium speed messages	Less than 100 ms	Yes
Type 3, Low speed messages	Less than 500 ms	Yes
Type 4, Raw data message, P1	In the order of 10 ms	Unlikely
Type 4, Raw data message, P2 and P3	In the order of 3 ms	No
Type 5, File transfer functions	No specific limits, typically equal to or greater than 1000 ms	Yes
Type 6, Time synchronization messages. Class T1	Accuracy +/- 1 ms	TBD
Type 6, Time synchronization messages. Class T2	Accuracy +/- 0.1 ms	TBD
Type 6, Time synchronization messages. Class T3	Accuracy +/- 25 us	TBD
Type 6, Time synchronization messages. Class T4	Accuracy +/- 4 us	TBD
Type 6, Time synchronization messages. Class T5	Accuracy +/- 1 us	TBD

Although it is possible to filter out message types that cannot be transported by WiMAX, the more that are filtered out the less the beneficial effectiveness of the WiMAX system, if message types 1A and 4 are excluded the following limits based on field test should enable the other message types to be transported by a WiMAX system.

Table 2: Latency limits without message types 1A and 4

Path with UGS service flows	Latency
CPE to base station	20 to 30 ms
Base station to CPE	20 to 30 ms
CPE to CPE, via the same or different base station	40 ms

2. Objective and Scope

Although WiMAX® profiles and other 802.16 variants currently available are being used or being considered for Smart Grid networks, it is clear that, although being an adequate solution compared to competing technologies, they are not an optimal solution for Smart Grid applications. The objective of this document is to define the requirements for new system profiles based on IEEE 802.16 that more closely meet or exceeds the utility end user requirements for AMI/Smart Grid broadband wireless networks. To differentiate these profiles from other WiMAX profiles these new profiles for Smart Grid applications will be referred to as WiGRID™ profiles.

The scope of the work item is as follows:

- To define the use cases for Smart Grid utility communications.
- To define the requirements for system profiles that meet the needs of Smart Grid utility communications

3. Abbreviations, Definitions, and Conventions *(Informative)*

This section includes acronyms, abbreviations, and definitions commonly encountered in Smart Grid related documents from NIST, SGIP, and OpenSG. Although not all of these terms relate directly to the task at hand, they are included here as an aid to those who may want to cross-reference this document with other Smart Grid documents published by other groups and organizations.

3.1 Abbreviations and Acronyms

ACK	Acknowledgement
AMI	Advanced Metering Infrastructure
AMS	Asset Management System
ARQ	Automatic Repeat-reQuest
ASAP-SG	Advanced Security Acceleration Project-Smart Grid
B2B	Business to Business
BAN	Business Area Network
BER	Bit Error Rate
BGAN	Broadband Global Area Network
CIM	Common Information Model
CIP	Critical Infrastructure Protection
CPP	Critical Peak Pricing
CRC	Cyclic Redundancy Check
CSWG	Cyber Security Working Group
DA	Distribution Automation
DAC	Distributed Application Controller
DAP	Data Aggregation Point
DCF	Distributed Coordination Function
DER	Distributed Energy Resources
DG	Distributor Generation
DHS	Department of Homeland Security3
DIFS	Distributed InterFrame Space
DL	Down-Link
DMS	Distribution Management System
DNP	Distributed Network Protocol
DO	Downlink Only
DOE	Department of Energy
DOMA	Distribution Operations Model and Analysis
DR	Demand Response
DRMS	Distribution Resource Management System

DSDR	Distribution Systems Demand Response
DSM	Demand Side Management
DVB	Digital Video Broadcast
EAG	Economic Area Grouping
EIFS	Extended InterFrame Space
EIRP	Effective Isotropic Radiated Power
EISA	Energy Independence and Security Act
EMS	Energy Management System
EPRI	Electric Power Research Institute4
ES	Electric Storage
ESB	Enterprise Service Bus
ESI	Energy Services Interface
ET	Electric Transportation
ETS	Emergency Telecommunication Services
EUMD	End Use Measurement Device
EV/PHEV	Electric Vehicle/Plug-in Hybrid Electric Vehicles
EVSE	Electric Vehicle Service Element
FAN	Field Area Network
FDD	Frequency Division Duplexing
FEP	Front End Processor
FER	Frame Error Rate
FERC	Federal Energy Regulatory Commission5
FIPS	Federal Information Processing Standard Document
FLIR	Fault Location, Isolation, Restoration
G&T	Generations and Transmission
GAPP	Generally Accepted Privacy Principles
GCC	Grid Control Center
GIS	Geographic Information System
GL	General Ledger
GMR	Geo Mobile Radio
GOOSE	Generic Object-Oriented Substation Event
HAN	Home Area Network
HARQ	Hybrid Automatic Repeat reQuest
HES	Head-End Server
HMI	Human-Machine Interface
HR	High Reliability
HVAC	Heating, Ventilating, and Air Conditioning

I2G	Industry to Grid
IEC	International Electrotechnical Commission6
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IHD	In-Home Display / In-Home Device
IKB	Interoperability Knowledge Base
IPoS	Internet Protocol over Satellite
ISO	Independent System Operator International Organization for Standardization
LAN	Local Area Network
LMS	Load Management System
LMS/DRMS	Load Management System/ Distribution Resource Management System
LV	Low Voltage
M2M	Machine to Machine
MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MDMS	Meter Data Management System
MEA	Major Economic Area
MFR	Multi-Feeder Reconnection
MIMO	Multiple-Input / Multiple-Output
MS	Mobile Station
MSW	Meter Service Switch
MV	Medium Voltage
NAN	Neighborhood Area Network
NERC	North American Electric Reliability Corporation8
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NLOS	Non Line of Sight
NMS	Network Management System
ODW	Operational Data Warehouse
OFDM	Orthogonal Frequency Division Multiplexing
OMS	Outage Management System
OpenSGug	Open Smart Grid Users Group
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PAP	Priority Action Plan
PCT	Programmable Communicating Thermostat

PEV	Plug-In Electric Vehicle
PGF	Probability Generating Function
PHEV	Plug-in Hybrid Electric Vehicle
PHY	Physical Layer
PI	Process Information
PIA	Privacy Impact Assessment
PII	Personally Identifying Information
PTT	Push to Talk
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RC	Regional Collector
REP	Retail Electric Provider
RSM	Regenerative Satellite Mesh
RSSI	Received Signal Strength Indication
RTO	Regional Transmission Operator
RTP	Real Time Pricing
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Development Organization
SG	Smart Grid
SGIP	Smart Grid Interoperability Panel
SIFS	Short InterFrame Space
SIM	Subscriber Identity Module
SIMO	Single-input / Multiple-output
SINR	Signal to Interference plus Noise Ratio
SISO	Single-input / Single-output
SM	Smart Meter
SNR	Signal to Noise Ratio
SSP	Sector-Specific Plans
TDD	Time Division Duplexing
TF	Task Force
TOU	Time Of Use
UCA	Utility Communications Architecture
UCAIug	UCA International Users Group
UL	Up-Link
VAR	Volt-Amperes Reactive
VVWS	Volt-VAR-Watt System

WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WASA	Wide Area Situational Awareness
WLAN	Wireless Local Area Network
WMS	Work Management System
WWAN	Wireless Wide Area Network

3.2 Definitions

Actor: A generic name for devices, systems, or programs that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems represent examples of devices and systems.

Anonymize: A process of transformation or elimination of personally identifiable information (PII) for purposes of sharing data

Aggregation: Practice of summarizing certain data and presenting it as a total without any personally identifiable information (PII) identifiers

Applications: Tasks performed by one or more actors within a domain.

Asset Management System: A system(s) of record for assets managed in the smart grid. Management context may change (e.g. financial, network).

Bird of the wire: A device for measuring voltage and current parameters that is fixed to a power transmission line and that is powered by the same power transmission line. The device is typically connected by wireless to a central device such that the bird on the wire device can either transmit information or receive instructions.

Capacitor Bank: This is a device used to add capacitance as needed at strategic points in a distribution grid to better control and manage volt-amperes reactive (VARs) and thus the power factor and they will also affect voltage levels.

Common Information Model: A structured set of definitions that allows different smart grid domain representatives to communicate important concepts and exchange information easily and effectively.

Common Web Portal: Web interface for regional transmission operator, customers, retail electric providers and transmission distribution service provider to function as a clearing house for energy information. Commonly used in deregulated markets.

Data Collector: See Substation controller

Data Aggregation Point (DAP): This device is a logical actor that represents a transition in most advanced metering infrastructure (AMI) networks between wide area networks and neighborhood area networks. (e.g. collector, cell relay, base station, access point, etc.)

De-identify: A form of anonymization that does not attempt to control the data once it has had personally identifiable information (PII) identifiers removed, so it is at risk of re-identification.

Demand Side Management: A system that co-ordinates demand response / load shedding messages indirectly to devices (e.g., set point adjustment)

Distributed Generation: These are facilities that generate power local to where power is consumed that can either be connected or isolated from the main power network based on the power demand.

Distribution Management System (DMS): A system that monitors, manages, and controls the electric distribution system.

Distribution Systems Demand Response (DSDR): A system used to reduce load during peak demand. Strictly used for distribution systems only.

Electric Vehicle (EV) /Plug-in Hybrid Electric Vehicles (PHEV): Cars or other vehicles that draw electricity from batteries to power an electric motor. PHEVs also contain an internal combustion engine.

Energy Services Interface (ESI): Provides the communications interface performing as a gateway to the utility or energy provider. It provides security and, often, coordination functions that enable secure interactions between relevant home area network devices and the utility. Permits applications such as remote load control, monitoring and control of distributed generation, in-home display of customer usage, reading of non-energy meters, and integration with building management systems. Also provides auditing/logging functions that record transactions to and from home area networking devices.

Enterprise Service Bus (ESB): The enterprise service bus consists of a software architecture used to construct integration services for complex event-driven and standards-based messaging to exchange meter or grid data. The enterprise service bus (ESB) is not limited to a specific tool set rather it is a defined set of integration services.

Fault Detector: A device used to sense a fault condition and can be used to provide an indication of the fault.

Field Force: Employee(s) working in the service territory that may be working with smart grid devices.

Generally Accepted Privacy Principles: Privacy principles and criteria developed and updated by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.

Goodput: Goodput is the application level throughput, i.e. the number of useful bits per unit of time forwarded by the network from a certain source address to a certain destination, excluding protocol overhead, and excluding retransmitted data packets.

Header: The portion of a packet, before the data field that typically contains source and destination addresses, control fields and error check fields.

Home Area Network: A network of energy management devices, digital consumer electronics, signal-controlled or enabled appliances, and applications within a home environment that is on the home side of the electric meter.

Intelligent Fault Detector: A device that can sense a fault and can provide more detailed information on the nature of the fault, such as capturing an oscillography trace.

Interoperability: The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user. The Smart Grid will be a system of interoperable systems. That is, different systems will be able to exchange meaningful, actionable information. The systems will share a common meaning of the exchanged information, and this information will elicit agreed-upon types of response. The reliability, fidelity, and security of information exchanges between and among Smart Grid systems must achieve requisite performance levels.

Interchangeability: An extreme degree of interoperability characterized by a similarity sometimes termed "plug and play." Interchangeable components can be freely substituted without loss of function and requiring minimal or no additional configuration.

ISO/IEC27001: Provides an auditable international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System within the context of the organization's overall business risks. It uses a process approach for protection of critical information

Last Gasp: Refers to the capability of a device to emit one last message when it loses power. Concept of an energized device within the smart grid detecting power loss and sending a broadcast message of the event

Latency: As used in the OpenSG – SG Communications SG Network TF's Requirement Table, is the summation of actor (including network nodes) processing time and network transport time measured from an actor sending or forwarding a payload to an actor, and that receiving actor processing (consuming) the payload. This "latency" is not the classic round trip "response time", or the same as "network link latency."

Link Budget: Accounts for the attenuation of the transmitted signal due to antenna gains, propagation, and miscellaneous losses.

Load Management System: A system that controls load by sending messages directly to device (e.g. On/Off)

Low Voltage Sensor: A device used to measure and report electrical properties (such as voltage, current, phase angle or power factor, etc.) at a low voltage customer delivery point.

Medium Voltage Sensor: A device used to measure and report electrical properties (such as voltage, current, phase angle or power factor, etc.) on a medium voltage distribution line.

Motorized Switch: A device under remote control that can be used to open or close a circuit

Neighborhood Area Network: A network comprised of all communicating components within a distribution domain.

Network Management System: A system that manages fault, configuration, auditing/accounting, performance and security of the communication. This system is exclusive from the electrical network.

Outage Management System: A system that receives out power system outage notifications and correlates where the power outage occurred

Packet: A formatted unit of data sent across a network.

Personal Information: Information that reveals details, either explicitly or implicitly, about a specific individual's household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual.

Phase or Phasor Measuring Unit: A device capable of measuring the phase of the voltage or current waveform relative to a reference.

Power Factor: A dimensionless quantity that relates to efficiency of the electrical delivery system for delivering real power to the load. Numerically, it is the cosine of the phase angle between the voltage and current waveforms. The closer the power factor is to unity the better the inductive and capacitive elements of the circuit are balanced and the more efficient the system is for delivering real power to the load(s).

Power quality: This is a term used to describe a number of parameters associated with electrical power, such as variations in level, changes in frequency, harmonics content, or transients,

Privacy Impact Assessment: A process used to evaluate the possible privacy risks to personal information, in all forms, collected, transmitted, shared, stored, disposed of, and accessed in any other way, along with the mitigation of those risks at the beginning of and throughout the life cycle of the associated process, program or system.

Programmable Communicating Thermostat: A device within the premise that has communication capabilities and controls heating, ventilation and cooling systems.

Rate Adaptation: The mechanism by which a modem adjusts its modulation scheme, encoding and/or speed in order to reliably transfer data across channel exhibiting different signal-to-noise ratio (SNR) characteristics.

Recloser (non-Team): A device used to sense fault conditions on a distribution line and trip open to provide protection. It is typically programmed to automatically close (re-close) after a period of time to test if the fault has cleared. After several attempts of reclosing it can be programmed to trip open and stop trying to reclose until reset either locally or under remote control.

Recloser (Team): A device that can sense fault conditions on a distribution line and to communicate with other related reclosers (the team) to sectionalize the fault and provide a coordinated open/close arrangement to minimize the effect of the fault.

Reference Model: A set of views (diagrams) and descriptions that provides the basis for discussing the characteristics, uses behavior, interfaces, requirements, and standards of the Smart Grid. This model does not represent the final architecture of the Smart Grid; rather it is a tool for describing, discussing, and developing that architecture.

Regional Transmission Operator: An organization that is established with the purpose of promoting efficiency and reliability in the operation and planning of the electric transmission grid and ensuring non-discrimination in the provision of electric transmission services based on the following required/demonstrable characteristics and functions.

Reliability: The ability of a system or component to perform its required functions under stated conditions for a specified period of time. It is often measured as a probability of failure or a measure of availability. However, maintainability is also an important part of reliability engineering.

Remote Terminal Unit: Aggregator of multiple serialized devices to a common communications interface

Smart Meter: Term applied to a 2-Way Meter (meter metrology plus a network interface component) with included energy services interface (ESI) in the meter component

Sub Meter: Premise based meter (e.g., used for Distributed Energy Resources and PHEV), which permits additional metering capabilities subordinate to a main meter.

Substation Controller: Distributed processing device that has supervisory control or coordinates information exchanges from devices within a substation from a head end server.

Throughput: The number of bits (regardless of purpose) moving over a communications link per unit of time. Throughput is most commonly expressed in bits per second.

Transformer (MV-to- LV): A standard point of delivery transformer. In the smart grid context it is assumed there will be a need to measure some electrical or physical characteristics of this transformer such as voltage (high and/or low side) current, MV load, temperature, etc.

Use Case: A systems engineering tool for defining a system's behavior from the perspective of users. In effect, a use case is a story told in structure and detailed steps—scenarios for specifying required usages of a system, including how a component, subsystem, or system should respond to a request that originates elsewhere.

Voltage Regulator: This device is in effect an adjustable ratio transformer positioned at strategic points in a distribution grid and is utilized to better manage and control the voltage as it changes along the distribution feeder.

Volt-Amperes Reactive: In an alternating current (AC) power system the voltage and current measured at a point along the delivery system will often be out of phase with each other as a result the combined effects of the resistive and reactive (i.e. the capacitance and inductive) characteristics of the delivery system components and the load. The phase angle difference at a point along the delivery system is an indication of how well the inductive and capacitive effects are balanced at that point. The real power passing that point is the product of the magnitude of the voltage and current and the cosine of the angle between the two. The VAR parameter is the product of the magnitude of the voltage and current and the sine of the angle between the two. The magnitude of the VAR parameter is an indication of the phase imbalance between the voltage and current waveforms.

Web Portal: Interface between customers and their smart grid service provider (e.g., utility or third party or both).

WiMAX/WiGRID service provider: A service provided either by the utility or third party of WiMAX or WiGRID based services.

3.3 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119]

From RFC2119 (For informative purposes):

1.MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3.SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

6. Guidance in the use of these Imperatives
Imperatives of the type defined in this memo must be used with care and sparingly. In particular, they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions) For example, they must not be used to try to impose a particular method on implementors where the method is not required for interoperability.

7. Security Considerations
These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.

4. References

[1] NISTIR 7761, NIST Priority Action Plan 2, Guidelines for Assessing Wireless Standards for Smart Grid Applications, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFNISTIR7761

[2] NISTIR-7628, Guidelines for Smart Grid Cyber Security, Volumes 1 and 2, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFNISTIR7628

[3] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[4] EISA Title XIII, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/EISA_Title_XIII_Smart_Grid.pdf

[5] IEEE Std 802.15.4g

[6] IEEE Std 802.16e-2009, IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems

[7] IEEE Std 802.16m, Amendment to IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems - Advanced Air Interface

[8] IEEE Std 802.16n, Higher Reliability Networks

[9] IEEE Std 802.16p, Enhancements to Support Machine-to-Machine Applications

5. Mapping WiMAX Forum System Profile Requirements for Smart Grid Applications to NIST-SGIP and the OpenSG Users Group

The development of a "Smart Grid" was established as a national policy goal in the United States with the Energy Independence and Security Act of 2007 (EISA). At that time the National Institute of Standards and Technology (NIST) was assigned the ***"primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of Smart Grid devices and systems…"*** (EISA Title XIII [4], Section 1305).

To facilitate its efforts, NIST created the Smart Grid Interoperability Panel (SGIP) in November 2009. The SGIP, under NIST oversight, was created to provide a framework to support stakeholder participation and representation to further the development and evolution of Smart Grid interoperability standards. As of September 2011 the SGIP membership includes 723 organizations representing 22 categories of Smart Grid stakeholders. Although US-centric, 85 SGIP member organizations are outside the US, thus ensuring international Smart Grid interests are represented. The WiMAX Forum is a participating SGIP member with emphasis on Priority Action Plan 2 (PAP02) which is responsible for the document NISTIR7761 [1] "Guidelines for Assessing Wireless Standards for Smart Grid Applications", Release 1 of this document was published in the middle of 2011[2] and release 2 is currently underway with a target completion in mid-2013.

Another key collaborative relationship exists between the NIST-SGIP and various working groups of Open Smart Grid (OpenSG) Users Group. Two of the OpenSG working groups, SG Communications and SG Security are especially relevant to wireless networks. The SG Communications Working Group is currently developing a detailed Smart Grid Network System Requirements Specification (SG NET SRS) for Smart Grid communication networks. Although this document is still work in process, the WiMAX Forum is actively engaged with the SG Communications working group to ensure consistency between these WiGRID specifications and the SG NET SRS

Another relevant document for the understanding of Smart Grid communications objectives is the "*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0"*.[3] [3] published in 2010. Release 2 of this framework document was drafted in July 2011 and will be published pending final review. This document is especially important in helping us understand the terminology, nomenclature, and definitions being adopted by the utilities community as driven by the SGIP and its members. As we move forward with the development of a WiGRID System Requirements specification it will be important to align our terminology with that of our end-customers, the utilities.

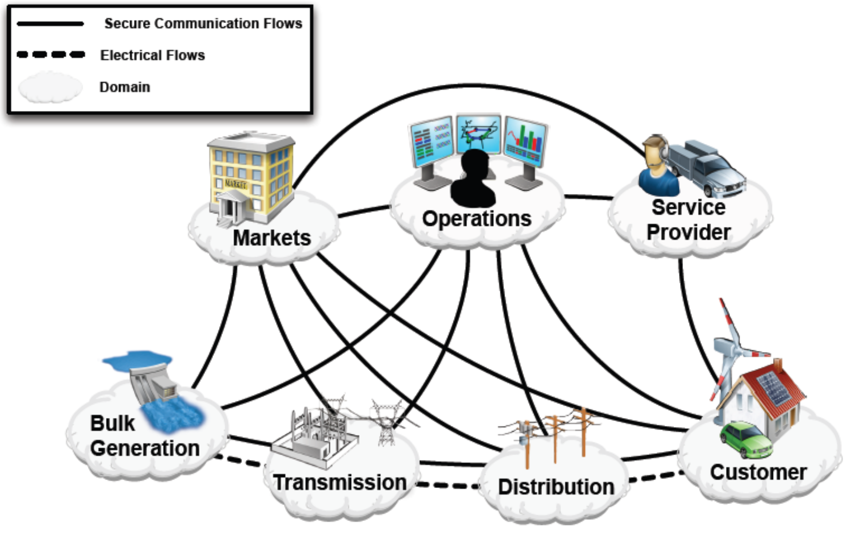
Much of the material following in this section is excerpted, with permission, from Release 2 of the NIST framework document.

NIST developed a conceptual model to support planning and organization of the diverse, expanding collection of interconnected networks that will compose the Smart Grid. For this purpose, NIST adopted the approach of dividing the Smart Grid into seven domains as shown graphically in Figure , and further described in Table 3.

Each domain—and its sub-domains—encompass Smart Grid ***actors*** and ***applications***. Actors include devices, systems, programs, and stakeholders that make decisions and exchange information necessary for performing applications: smart meters, solar generators, and control systems are examples of devices and systems. These descriptions of the actors, applications, and requirements for communications that enable the functionality of the Smart Applications are tasks performed by one or more actors within a domain. For example, corresponding applications may be home automation; solar energy generation and energy storage; and energy management.

[2] https://collaborate.nist.gov/twiki sggrid/pub/SmartGrid/PAP02Objective3/NIST_PAP2_Guidelines_for_Assessing_Wireless_Standards_for_Smart_Grid_Applications_1.0.pdf

[3] http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf



NIST Smart Grid Framework

Figure 6 – SG Requires Secure Communications Between Actors in Different Domains

Table 3: Domains and Actors in the Smart Grid Conceptual Model

	Domain	Actors in the Domain
1	Customer	The end users of electricity. May also generate, store, and manage the use of energy. Traditionally, three customer types are discussed, each with its own domain: residential, commercial, and industrial.
2	Markets	The operators and participants in electricity markets.
3	Service Provider	The organizations providing services to electrical customers and utilities.
4	Operations	The managers of the movement of electricity.
5	Bulk Generation	The generators of electricity in bulk quantities. May also store energy for later distribution.
6	Transmission	The carriers of bulk electricity over long distances. May also store and generate electricity.
7	Distribution	The distributors of electricity to and from customers. May also store and generate electricity.

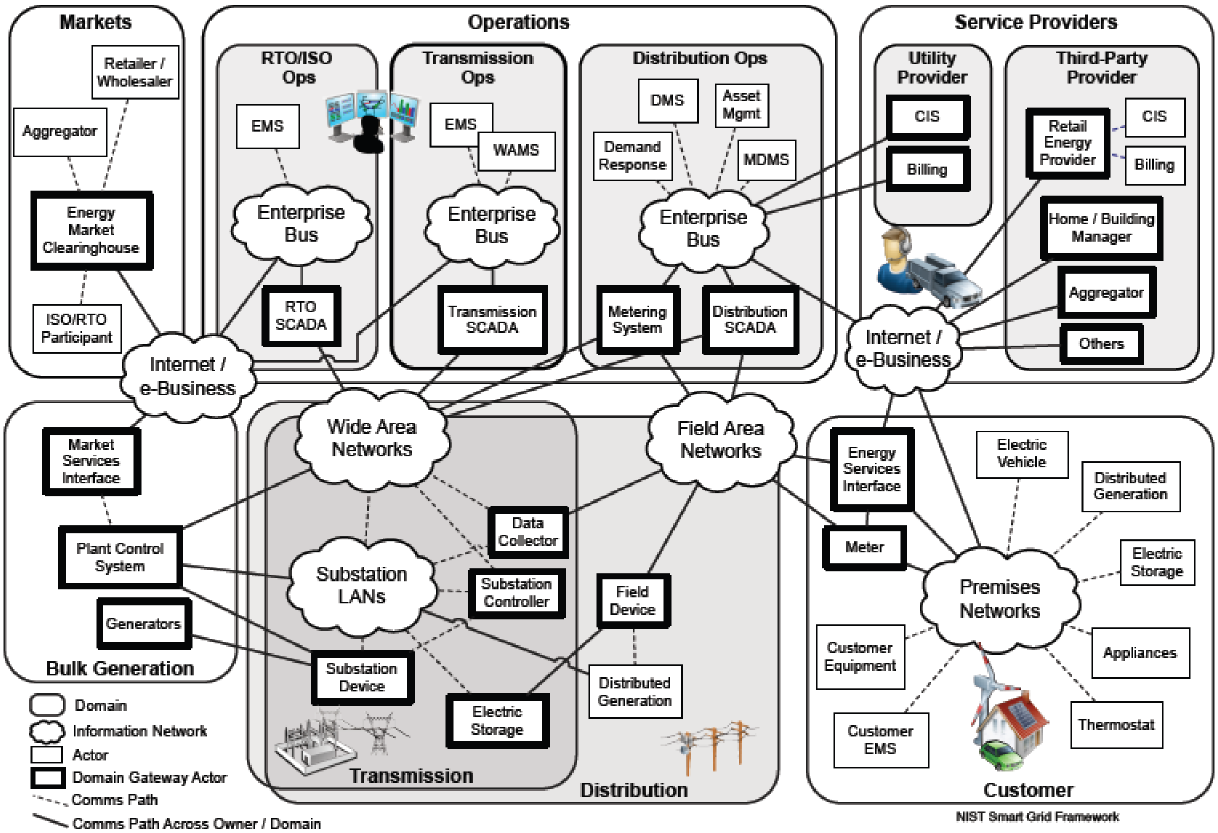


Figure 7 – Conceptual Reference Diagram for Smart Grid Information Networks

The NIST-SGIP Conceptual Reference Diagram provides further detail for the Smart Grid communications network.

- **Domain:** Each of the seven Smart Grid domains is a high-level grouping of organizations, buildings, individuals, systems, devices or other actors that have similar objectives and that rely on—or participate in—similar types of applications. Communications among actors in the same domain may have similar characteristics and requirements. Domains may contain sub-domains. Moreover, domains have much overlapping functionality, as in the case of the transmission and distribution domains. Transmission and distribution often share networks and, therefore, are represented as overlapping domains.
- **Actor:** An actor is a device, computer system, software program, or the individual or organization that participates in the Smart Grid. Actors have the capability to make decisions and to exchange information with other actors. Organizations may have actors in more than one domain. The actors illustrated here are representative examples but are by no means all of the actors in the Smart Grid. Each actor may exist in several different varieties and may actually contain other actors within them.
- **Gateway Actor:** An actor in one domain that interfaces with actors in other domains or in other networks. Gateway actors may use a variety of communication protocols; therefore, it is possible that one gateway actor may use a different communication protocol than another actor in the same domain, or may use multiple protocols simultaneously.
- **Information Network:** An information network is a collection, or aggregation, of interconnected computers, communication devices, and other information and communication technologies. Systems in a network exchange information and share resources. The Smart Grid consists of many different types of networks, not all of which are shown in the diagram. The networks include: the Enterprise Bus that connects control center applications to markets and generators, and with each other; ***Wide Area Networks*** that connect geographically distant sites; ***Field Area Networks*** that connect devices, such as Intelligent Electronic Devices (IEDs) that control circuit breakers and transformers; and ***Premises Networks or Home Area Networks*** that include customer networks as well as utility networks within the Customer domain.

These networks may be implemented using a combination of public (e.g., the Internet) and nonpublic networks. Both public and nonpublic networks will require implementation and maintenance of appropriate security and access control to support the Smart Grid. Examples of where communications may go through the public networks include: customers to third-party providers; bulk generators to grid operators; markets to grid operators; and third-party providers to utilities.

- **Communications (Comms) Path:** The communications path shows the logical exchange of data between actors or between actors and networks.

To prioritize its work, NIST chose to focus on six key functionalities or ***Use Cases*** plus ***Cyber-security and Network Communications***. These functionalities are especially critical to ongoing and near-term deployments of Smart Grid technologies and services and include the priorities recommended by the Federal Energy Regulatory Commission (FERC) in its policy statement[4]: A ***Use Case*** is essentially a story, told in structured and detailed steps, about how actors work together to reach a goal.

The Six NIST Priority Use Cases Are:

1. **Demand response and consumer energy efficiency:** Mechanisms and incentives for utilities, business, industrial, and residential customers to cut energy use during times of peak demand or when power reliability is at risk. Demand response is necessary for optimizing the balance of power supply and demand.

2. **Wide-Area Situational Awareness (WASA):** Monitoring and display of power-system components and performance across interconnections and over large geographic areas in near real time. The goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise.

3. **Energy Storage:** Means of storing energy, directly or indirectly. The most common bulk energy storage technology used today is pumped hydroelectric storage technology. New storage capabilities—especially for distributed storage—would benefit the entire grid, from generation to end use.

4. **Electric Transportation:** Refers, primarily, to enabling large-scale integration of plug-in electric vehicles (PEVs). Electric transportation could significantly reduce U.S. dependence on foreign oil, increase use of renewable sources of energy, and dramatically reduce the nation's carbon footprint.

5. **Advanced Metering Infrastructure (AMI):** Provides real-time monitoring of power usage, and is a current focus of utilities. These advanced metering networks are of many different designs and could also be used to implement residential demand response including dynamic pricing. AMI consists of the communications hardware and software, and the associated system and data management software, that together create a two-way network between advanced meters and utility business systems, enabling collection and distribution of information to customers and other parties, such as the competitive retail supplier or the utility itself. Because the networks do not share a common format, NIST is focusing on standardizing the information data models.

6. **Distribution Grid Management:** Focuses on maximizing performance of feeders, transformers, and other components of networked distribution systems and integrating with transmission systems and customer operations. As Smart Grid capabilities, such as AMI and demand response, are developed, and as large numbers of distributed energy resources and plug-in electric vehicles (PEVs) are deployed, the automation of distribution systems becomes increasingly more important to the efficient and reliable operation of the overall power system. The anticipated benefits of distribution grid management include increased reliability, reductions in peak loads, and improved capabilities for managing distributed sources of renewable energy. [5]

[4] http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf

[5] National Institute of Standards and Technology United States Department of Commerce. (2010 July). *Smart Grid Architecture and Standards: Assessing Coordination and Progress*. http://www.nist.gov/director/ocla/testimony/upload/DOC-NIST-testimony-on-Smart-Grid-FINAL-with-bio.pdf.

Other NIST priority functionalities include:

- **Cybersecurity:** Encompasses measures to ensure the ***confidentiality, integrity, and availability*** of the electronic information communication systems and the control systems necessary for the management, operation, and protection of the Smart Grid's energy, information technology, and telecommunications infrastructures. [6]

- **Network Communications:** This refers to a variety of public and private communication networks, both wired and wireless that will be used for Smart Grid domains and sub-domains. Given this variety of networking environments, the identification of performance metrics and core operational requirements of different applications, actors, and domains—in addition to the development, implementation, and maintenance of appropriate security and access controls—is critical to the Smart Grid. FERC notes, a "… cross-cutting issue is the need for a common semantic framework (i.e., agreement as to meaning) and software models for enabling effective communication and coordination across inter-system interfaces. An interface is a point where two systems need to exchange data with each other; effective communication and coordination occurs when each of the systems understands and can respond to the data provided by the other system, even if the internal workings of the system are quite different."[7]

Network security is a critical requirement to ensure that the ***confidentiality, integrity, and availability*** of Smart Grid information, control systems, and related information systems are properly protected.

Given the diversity of the networks, systems, and energy sectors involved, ensuring adequate security is critical so that a compromise in one system does not compromise security in other, inter-connected systems. A security compromise could impact the availability and reliability of the entire electric grid. In addition, information within each specific system also needs to be protected. Security includes the ***confidentiality, integrity, and availability (CI&A)*** of all related systems. The OpenSG Security Working Group is currently identifying and assessing the Smart Grid logical interfaces to determine the impact of a loss of confidentiality, integrity, or availability. The objective is to select security requirements to mitigate the risk of cascading security breaches.

A key document published by NIST SGIP in conjunction with OpenSG Security working group is ***NISTIR 7628 "Guidelines for Smart Grid Cyber Security: Volume 1 and Volume 2"***[8]**.**

Following are the definitions for the security objectives of CI&A, as defined by statute.

- **Confidentiality**: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…." [44 U.S.C., Sec. 3542] A loss of *confidentiality* is the unauthorized disclosure of information.

- **Integrity:** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…." [44 U.S.C., Sec. 3542] A loss of *integrity* is the unauthorized modification or destruction of information.

- **Availability:** "Ensuring timely and reliable access to and use of information…." [44 U.S.C., SEC. 3542] A loss of *availability* is the disruption of access to or use of information or an information system.

Based on these definitions, impact levels for each security objective (confidentiality, integrity, and availability) are specified as low, moderate, and high as defined in FIPS 199, *Standards for Security Categorization of Federal*

[6] National Institute of Standards and Technology United States Department of Commerce. (2010 July). *Smart Grid Architecture and Standards: Assessing Coordination and Progress*. http://www.nist.gov/director/ocla/testimony/upload/DOC-NIST-testimony-on-Smart-Grid-FINAL-with-bio.pdf.

[7] Proposed Policy Statement, 126 FERC ¶ 126, at p. 32.

[8] https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/NISTIR_7628_Assessment_Guide-v1p0-24Aug2012.pdf

Information and Information Systems, February 2004. The impact levels are used in the selection of security requirements for each logical interface category.

Table 4: Potential Impact Levels

	Potential Impact Levels		
	Low Priority (L)	**Moderate Priority (M)**	**High Priority (H)**
Confidentiality	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Impact on WiMAX Forum® System Profile Requirements for Smart Grid Applications:

Varied Use Cases and Sub-Use Cases will have varied requirements for Confidentiality, Integrity and Availability. In developing WiGRID requirements for Smart Grid applications it will be desirable to quantify these requirements through further interaction with the Utilities Community.

6. Utility Network Architectures

Utility Networks have a variety of 4G Core Network Architectures, depending on the applications they support. These networks range from simple Layer 2 networks, to complex networks that contain functionality from Layer 1-7 of the ISO Stack.

The networks considered in this requirements specification include the following options;

- Centralized: ASN-GW "Profile C" providing services using IP-CS or ETH-CS
- Distributed: ASN-GW "Profile B" providing services with IP-CS or ETH-CS
- Edge Router functions in Base Station providing services with ETH-CS
- Combinations of Networks with both ASN-GWs and Edge Router functions

A generic 4G Core Network Architecture is shown is the diagram below. Utility Core Networks can support both 4G WiMAX and 4G LTE functions.

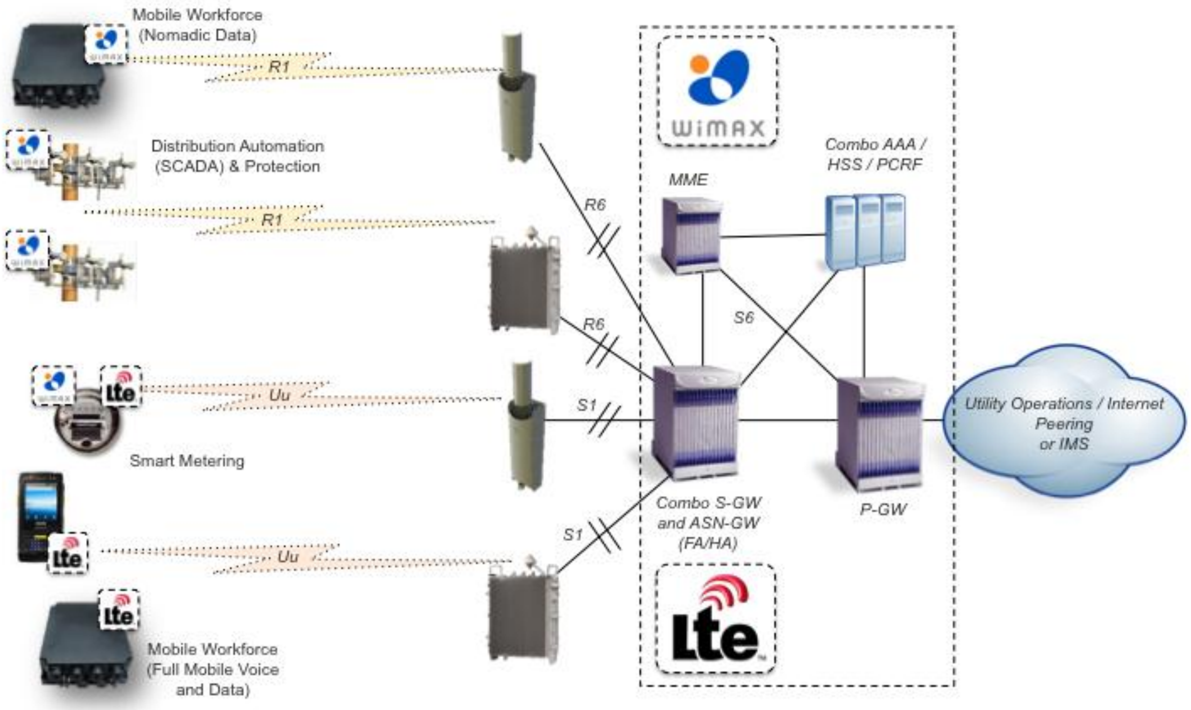

Mobile Workforce (Nomadic Data)
R1
Distribution Automation (SCADA) & Protection
R1
Smart Metering
Uu
Uu
Mobile Workforce (Full Mobile Voice and Data)
R6
R6
S1
S1
WiMAX
MME
Combo AAA / HSS / PCRF
S6
Combo S-GW and ASN-GW (FA/HA)
P-GW
Utility Operations / Internet Peering or IMS
Lte

Figure 8 – Utility Network Architectures

For the purposes of dimensioning the communication requirements of a Utility Network a number of connectivity scenarios should be considered.

6.1 Option 1: Layer 2 Networks using ETH-CS (WiMAX No-ASN-GW)

The simplest network does not require the ASN-GW function from a WiMAX/WiGRID CSN. In this architecture traffic from the radio interface is terminated at the base station (using an integral Edge router) capability.

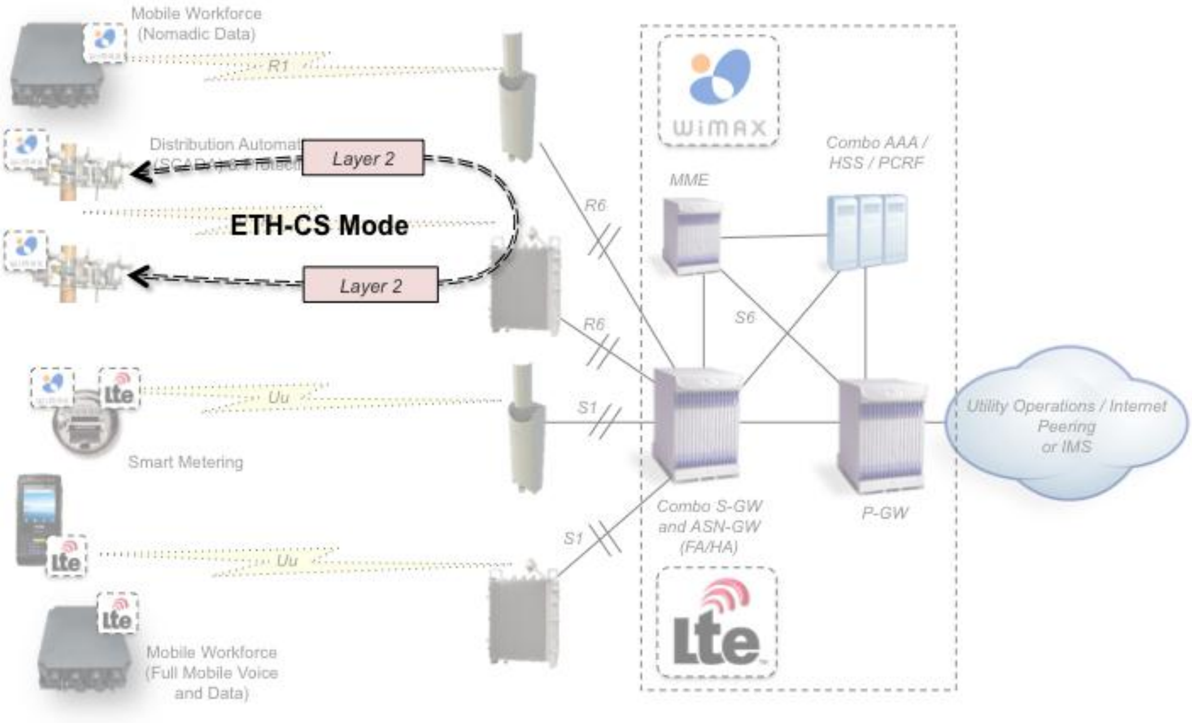

Mobile Workforce (Nomadic Data)
R1
Distribution Automat
Layer 2
ETH-CS Mode
Layer 2
Uu
Smart Metering
Uu
Mobile Workforce (Full Mobile Voice and Data)
R6
R6
S1
S1
WiMAX
MME
Combo AAA / HSS / PCRF
S6
Combo S-GW and ASN-GW (FA/HA)
P-GW
Utility Operations / Internet Peering or IMS
Lte

Figure 9 – Layer 2 Networks using ETH-CS

This type of network is often used to support applications like GOOSE messaging for Protection applications. Traffic can switched at the base station location without transiting the Core Network.

6.2 Option 2: Layer 2 and 3 Networks using IP-CS (WiMAX ASN-GW)

Some applications require the use of an ASN-GW function from a WiMAX/WiGRID CSN. Feature like Sleep and Idle mode for Direct to the Meter, Smart Metering, and applications like Handover for Mobile Workforce require the use of an ASN-GW.

These networks typically operate using IP-CS, and can also tunnel ETH-CS over IP-CS if Layer 2 functionality is required. The key architectural difference is that all traffic transits the ASN-GW function in the CSN (even if the connectivity is between CPEs on the same base station).

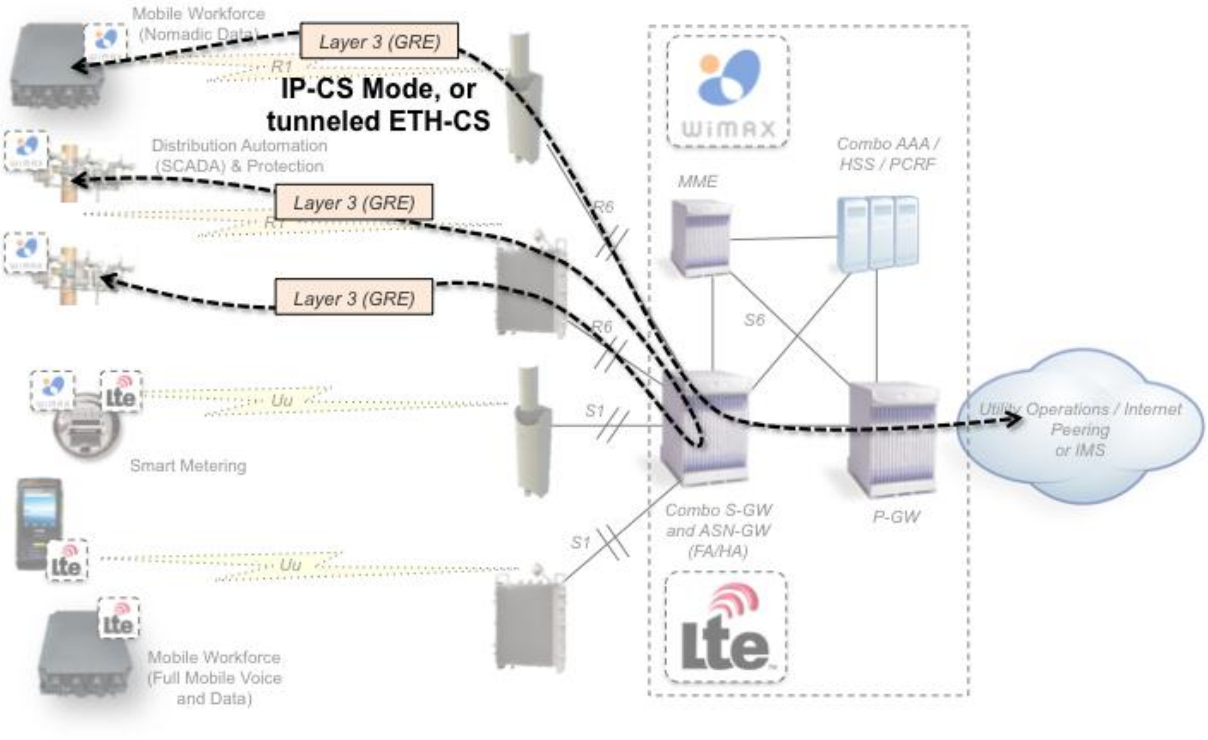


Figure 10 – Layer 2 and 3 Networks using IP-CS

6.3 Option 3: Layer 1-7 Networks using LTE

For completeness, it should be noted that many 4G Core Networks can support LTE and WiMAX/WiGRID simultaneously. LTE may be used by a utility for certain applications (for example Voice using VoLTE). These networks require all traffic to transit the S-GW (and most traffic via the P-GW).

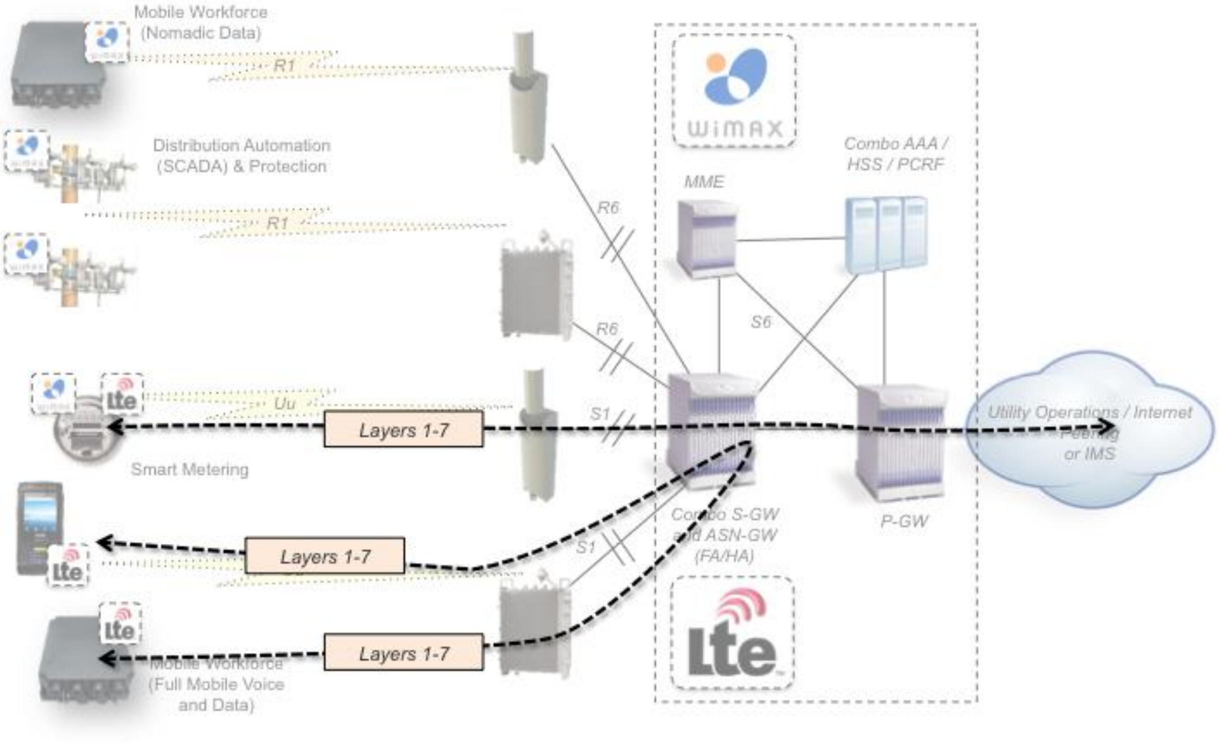


Figure 1 – Layer 1-7 Networks using LTE

Based on the efforts of NIST-SGIP and the OpenSG Users group there is clearly an expectation that multiple networks and types of networks will be required to fully meet the communications requirements for a fully functional Smart Grid. Additionally, utilities already have pre-existing communications networks that will remain in place as new networks are added. Although WiMAX and WiGRID Systems have the potential to fulfill requirements for a wide range of SG communications segments, realistically it can be expected that more than one wireless technology will be employed. Inter-network and inter-technology interworking will be necessary to ensure seamless actor to actor connectivity for all use cases.

7. Smart Grid Security Requirements

The SGIP Cyber Security working group has spent considerable effort in their attempt to address Cyber security and especially the privacy concerns relating to Smart Grid. The work of this group has been published in the previously referenced report, NISTIR-7628 [2], "Guidelines for Smart Grid Cyber Security, Volumes 1 and 2". Security breaches of a Smart Grid communications network can be initiated by a wide range of adversaries, some of whom may wish to create major service disruptions or even shut down the grid entirely and others that are only interested in creating a nuisance. From a customer perspective, if the network is not viewed as being secure, customers will be reluctant participate even though there may be financial incentives to do so.

From a security viewpoint, the Smart Grid communications network will be counted on to provide a level of defense beyond what today's conventional cellular networks can provide. Protections are required to prevent malicious attacks on the grid itself plus preventing unwanted access to sensitive utility and customer information. A wireless communications network is generally viewed as more vulnerable to security breaches and therefore WiGRID for Smart Grid applications must incorporate all available safeguards.

The IEEE working groups for the 802.16n [8] and 802.16p [9] amendments are also addressing Smart Grid security concerns. Security features developed for these two amendments should be considered for WiGRID profiles for Smart Grid applications. The following is from the Smart Grid Cyber Security report and is provided here to provide a better understanding of the security issues from SGIP's perspective.

The potential adversaries identified in Volume 1 of the above report are listed and described in the following table:

Table 5: List of potential adversaries

Adversary	Description
Nation States	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or a political advantage.
Hackers	A group of individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyber-terrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals with the potential to inflict harm on the Smart Grid network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or Poorly Trained Employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to Smart Grid systems. This is another

	example of an insider threat or adversary.

The following material is excerpted from Volume 2 [2] entitled "Privacy and the Smart Grid" and provides some insight as to privacy concerns that probably go beyond what is currently included with today's WiMAX and other cellular networks.

> *"….there is a wide range of privacy concerns to address within the Smart Grid. These may impact the implementation of Smart Grid systems or their effectiveness. For example, a lack of consumer confidence in the security and privacy of their energy consumption data may result in a lack of consumer acceptance and participation, if not outright litigation. In general, privacy concerns about the Smart Grid fall into one of two broad categories:*
>
> - *Type I: Personal information not previously readily obtainable; and*
> - *Type II: Mechanisms for obtaining (or manipulating) personal information that did not previously exist.*
>
> *Examples of Type I concerns include detailed information on the appliances and equipment in use at a given location, including the use of specific medical devices and other electronic devices that indicate personal patterns and timings of legal and potentially illegal operations within the location, and finely grained time series data on power consumption at metered locations and from individual appliances.*
>
> *Type II concerns include instances where personal information is available from other sources, and the Smart Grid may present a new source for that same information. For example, an individual's physical location can be tracked through their credit card and cell phone records today. Charging PEVs raises the possibility of tracking physical location through new energy consumption data. Detailed pictures of activities within a house or building can be derived from "equipment electricity signatures" and their time patterns. Such signatures and patterns can provide a basis for making assumptions about occupant activities (e.g., the number of individuals at a location and when the premise was unoccupied). While technology to communicate directly with appliances and other energy consumption elements already exists, Smart Grid implementation may create broader incentives for their use. Appliances so equipped may deliver detailed energy consumption information to both their owners and operators—and to outside parties."*

The report goes on to identify some of the ways for which data collection can be used. Although many uses may be to the consumers benefit some data may be used for purposes that violate an individual's right to privacy. Some examples of data that might be used for good or illicit purposes include:

- Electric usage data, when collected and analyzed over a period of time, can be used to determine occupant activities and lifestyle. For example, a forecast may be made about the number of individuals at a premise, when the location is unoccupied, sleep schedules, work schedules, and other personal routines.
- Granular Smart Grid data may provide assumptions about the health of a dwelling's resident in which some insurance companies, employers, newspapers (with regard to public figures), civil litigants, and others could be interested. As an example, specific medical devices may be uniquely identified through serial numbers or MAC addresses, or may have a unique electrical signature; either could indicate that the resident suffers from a particular disease or condition that requires the use of the device.
- Inferences might be used to determine health patterns and risk. For example, the amount of time the computer or television is on could be compared to the amount of time the treadmill is used.

Section 5.6.2 of Volume 2 speaks directly to the use of Wireless access. It states:

> *"Future designs for some smart meters and many secondary devices (e.g., appliances and smaller devices) may incorporate wireless-enabled technology to collect and transmit energy usage information for homes or businesses. Should designers and manufacturers of smart meters or secondary devices decide to incorporate wireless technology for the purpose of communicating energy usage information, then that data must be securely transmitted and have privacy protection. If in the future wireless technology is used*

> *to transmit aggregate home or business energy consumption information for a unique location or dwelling, then that usage data, prior to sufficient aggregation to protect privacy, should also be protected from unauthorized use, modification, or theft. There are well-known vulnerabilities related to wireless sensors and networks, and breaches of wireless technology. For example, "war driving" is a popular technique used to locate, exploit, or attack insufficiently protected wireless systems. Readily available portable computing devices are used to detect signals emanating from wireless technology."*

Unfortunately NISTIR-7628 [2] fails to indicate specific quantifiable security requirements for wireless Smart Grid networks. It is clear however, from the above cyber security and privacy issues and concerns raised by the SGIP Cyber Security Working Group that utilities network planners will pay close attention to what alternative technologies offer with respect to network security. It is imperative therefore, that WiGRID system profiles for Smart Grid emphasize and take advantage of the most advanced security features included in IEEE std 802.16e-2009 [6] and planned for in the 802.16n [8] and 802.16p amendments [9].

8. Utility Application Traffic Profiles

The Use Cases considered in this document are tabularized in the table below. The purpose of this table is to characterize the typical communication requirement for each type of application.

The table captures for the downlink (DL) and uplink (UL) the following key parameters;

- Latency
- Traffic Bandwidth (kbit/s)
- Packets per second
- Traffic (Message) Frequency
- Traffic Payload Type (TCP/UDP)
- QoS Type (Real-time, BE, UGS)
- Active / Idle Ratio
- Traffic activity predictability (Random, Regular)

Table 6: Utility Use Case: Communications Requirement Summary

Use Case	DL (kbit/s)	UL (kbit/s)	Latency (ms)	Packets per Sec	Msg. Freq.	Payload Type	Active / Idle	Predictability
1 – Situational Awareness (WASA)	1.0	5.0	1000	5pps	5sec	TCP	1sec / 5sec	Good
2 – Monitoring	~10	~300	100	100pps	100ms	TCP and UDP	Active	Good
3 – Control	1.0	5.0	100	10pps	1sec	TCP	1sec / 5sec	Random
4 – Protection	150	150	20	100pps	100ms	UDP	Active	Random
5 – Metering Regional Collector (DAP)	5	64	1000	20pps	100ms	TCP	Active	Good
6 – Remote Site Communications	500	500	100	100pps	20ms	TCP	Active	Good
7 – Direct 4G Smart Metering (AMI)	0.05	1.0	5000	1pps	5min to 6hr	TCP	100ms / 4sec	Good

9. Utility Frequency Bands

9.1 Utility Frequency Bands in the US

Utilities in the USA have limited access to licensed or lightly licensed spectrum. The bands available for "Private 4G" deployment are limited to a few choices. It is important that these options are included in any WiMAX Forum Smart Grid System Profile.

9.1.1 2.3 GHz – WCS Band, C & D Blocks

The 2.3 GHz WCS band in the US is made up of two 15 MHz spectrum blocks (2305-2320 MHz and 2345 -2360 MHz), which surround the 25 MHz satellite digital audio radio service (SDARS) band. The 30 MHz in the WCS is further subdivided into four sub-blocks

- A and B Blocks each with 10 MHz of paired spectrum (2x5 MHz)
- C and D Blocks each with 5 MHz unpaired spectrum

The C and D Blocks are potentially available to Utilities for deployment for Smart Grid applications.

The C and D Blocks are defined as 2315 MHz to 2320 MHz and 2345 to 2350 MHz respectively.

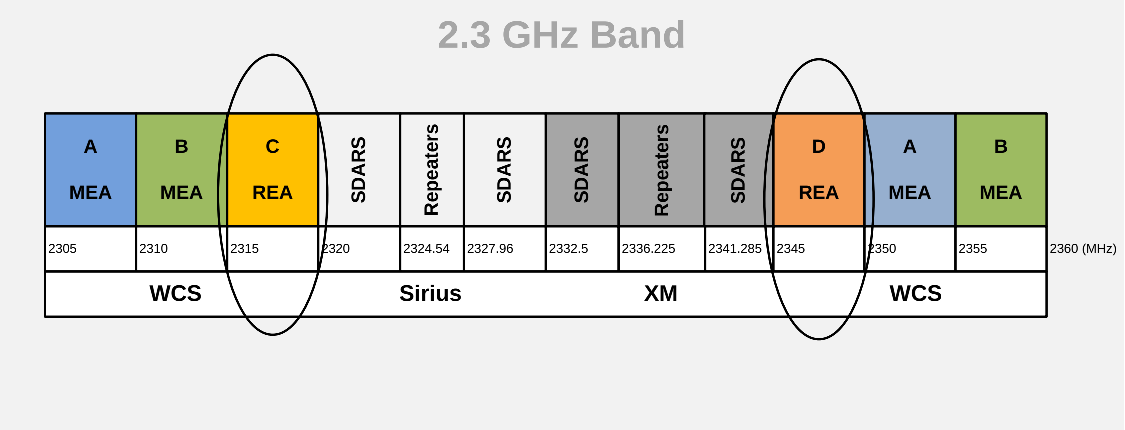


Figure 2 – 2.3 GHz Spectrum Allocation

The challenge with the 2.3 GHz C&D Blocks is to meet the stringent block-edge emissions which requires aggressive filtering. This filtering requirement typically prevents the use of 5 MHz channel bandwidths.

In addition to the filtering requirement, Mobility and Portable operation is prohibited in the 2.5 MHz closest to the SDARS. To enable Utilities to support Mobile and Portable operation, 2.5 MHz channels bandwidth is required.

Therefore;

> to enable effective use of 2.3 GHz C&D Blocks it is proposed that the Smart Grid (WiGRID) System Profiles MUST support 3.5 MHz TDD channels, MAY support 3.0 MHz TDD channels.

9.1.2 3.65 GHz – FCC 3650-3700 MHz

The band 3650 MHz to 3700 MHz is available in the USA on a semi-licensed basis. Registration with the FCC is mandated and a record is kept of all deployments in the band.

A large number of US Utilities have deployed solutions at 3.65 GHz.

This band is ideal for fixed applications and some nomadic applications.

Many vendors already have 802.16e [6] WiMAX solutions available in this band.

Some areas in the USA are excluded. These are shown in the diagram below.

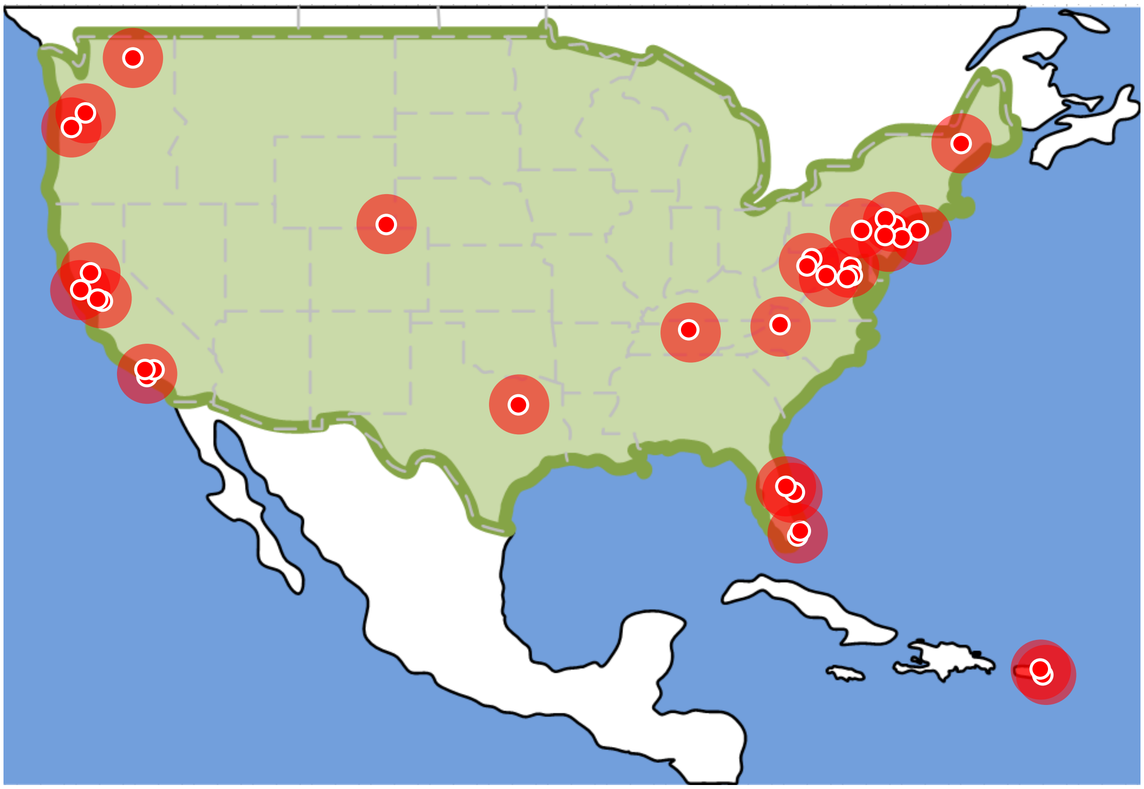


Figure 3 – 3.65 GHz Spectrum Allocations in the USA

Therefore;

to enable effective use of the 3.65 GHz spectrum allocation it is proposed that the Smart Grid (WiGRID) System Profiles MUST support 5 MHz and 10 MHz TDD channels and MAY support 3.0 MHz, and 7 MHz TDD channels.

9.1.3 1.4 GHz – 1390 MHz to 1395 MHz and 1432 MHz to 1435 MHz

The 1.4 GHz allocation in the USA (1390 MHz to 1395 MHz and 1432 MHz to 1435 MHz) may be available to Utilities for lease (First Energy). The leases permit up to 8 MHz to be allocated to a Utility in its service area (consisting of a 3 MHz + 5 MHz allocation). It is considered very unlikely that the spectrum will be disaggregated into blocks as originally defined by the FCC (see figure 13) . The spectrum can support either TDD or FDD.

An allocation in the UK (1427 MHz to 1452 MHz) exists and the coordinating body for UK utilities has negotiated access for an operational pilot and potential commercial deployment in 2013.

To enable effective use of this band custom 802.16e [6] channel sizes are required. In the US this is partly driven by the current rules that govern FCC certification, namely Part 27.50, 27.52, 27.53, and 27.55. In the UK this is driven by the need to coordinate with other primary users (namely the UK Ministry of Defence).

In the US the current FCC rules, Part 27.53 (j) on emission limits, do not provide any significant adjacent channel relief and enforce a strict observation of 43 dB+10Log(P)/1MHz = -13 dBm/1MHz. Therefore, for a Base Station or Device to meet these requirements 3 MHz and 5 MHz channel sizes are required.

In the UK standard WiMAX channel sizes can be utilized.

Therefore;

to enable effective use of the 1.4 GHz spectrum allocations it is proposed that the Smart Grid (WiGRID) System Profiles MUST support 3.0 MHz TDD channel in 1390-1395 MHz band and MUST support 3.0 MHz TDD channels in 1432 – 1435 MHz and SHOULD support paired 3.0 MHz channels for FDD operation in 1392 – 1435 MHz band and SHOULD support 5.0 MHz channels in the 1390-1395 MHz band.

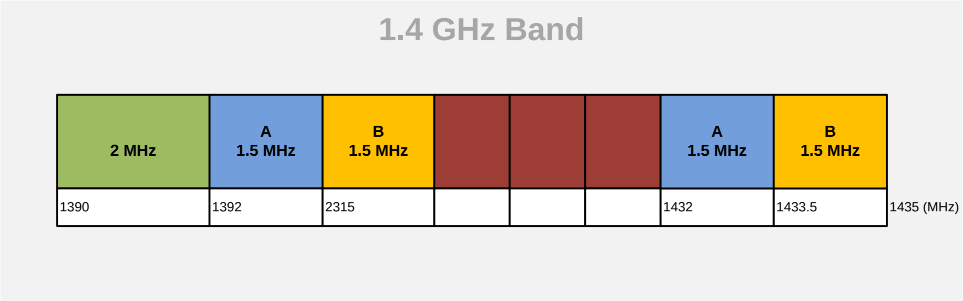


Figure 4 – 1.4 GHz Spectrum Allocation

Table 7: List of frequency blocks

Block	Frequencies	Bandwidth	Pairing	Geo. Type Area	No. of Licenses
	1390-1392	2 MHz	Unpaired	MEA	52
A	1392-1393.5 1432-1433.5	3 MHz	2 x 1.5 MHz	EAG	6
B	1393.5-1395 1433.5-1435	3 MHz	2 x 1.5 MHz	EAG	6

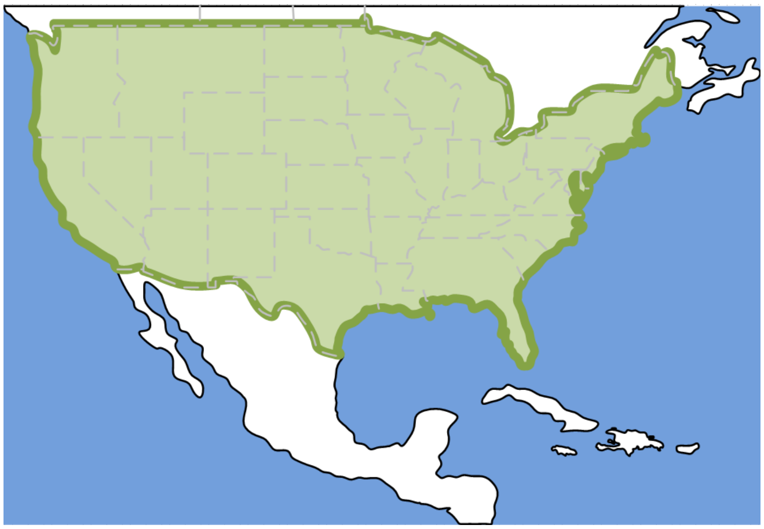


Figure 5 – 1.4 GHz Spectrum Allocations in the USA

9.2 Utility Frequency Bands in Canada

Electricity Utilities in the Canada have access to licensed spectrum in the 1800 to 1830 MHz band.

This allocation is for specific deployment scenarios and applications for radio systems for operations, maintenance and management of the electricity supply. Industry Canada has a set of technical requirements for these systems which are as follows:

- Fixed Services only
- Minimum antenna gain of 12 dBi for remote and 11 dBi for central stations.
- Maximum value of the transmitted power level (EIRP) of +13 dBW.

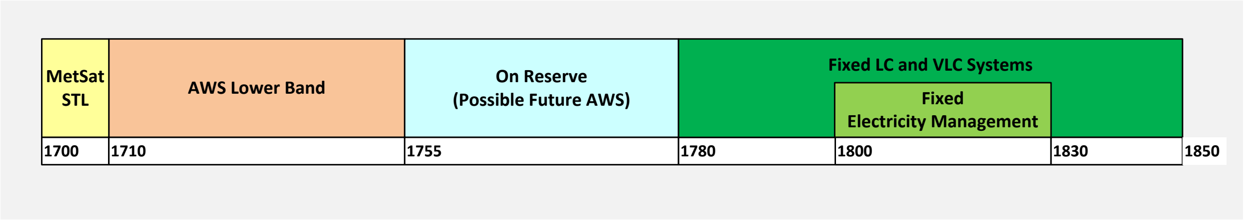


Figure 6 – Frequency Bands in Canada

9.2.1 Radio Frequency Channel Arrangements

A range of bandwidths are available permissible, centre frequencies may be assigned on a 125 kHz grid. Channel bandwidths of 1 to 10 MHz in 250 kHz increments may be assigned as needed in the band.

Systems used for the management of the electricity supply in the band 1800-1830 MHz, the transmitter power delivered to the antenna input shall not exceed 2 watts (3 dBW or 33 dBm) in any 1 MHz segment within the channel bandwidth.

The center frequency of the emission shall be maintained within ±0.001% of the assigned frequency for digital systems.

For systems used for the management of the electricity supply in the band 1800 – 1830 MHz, the unwanted emissions of transmitters of base stations and terminals shall be attenuated below the transmitter power, P, measured in watts, by no less than 43 + 10 log (P), dB.

The unwanted emission power shall be measured with a resolution bandwidth of 1 MHz. However, in the 1 MHz band immediately outside and adjacent to the equipment channel, a resolution bandwidth of at least 1% of the emission bandwidth shall be employed. A narrower resolution bandwidth is allowed to be used provided the measured power is integrated over the full required measurement bandwidth of 1 MHz or 1% of the emission bandwidth, as applicable.

The gain of the base station antennas must exceed 11 dBi. Omnidirectional antennas are permitted; however, the use of directional antennas is encouraged to reduce interference and facilitate network planning.

The gain of the terminal station antennas must exceed 12 dBi. The 3 dB beam width shall not exceed 30 degrees in vertical and horizontal polarizations, and the front-to-back ratio shall be greater than 20 dB.

“Industry Canada allows the use of the frequency band from 1800 to 1830 MHz for power management system, the regulation SRSP 301.7 details the conditions of use of the band. From the frequency range of 1800 to 1830 MHz, a utility can be assigned up to 20 MHz, additional assignments are based on a technical justification being provided.

A requirement of the assignment is that co-ordination is required for co-existence with system deployed in the United States.”[9]

Therefore;

to enable effective use of the 1800 MHz spectrum allocation it is proposed that the Smart Grid (WiGRID) System Profiles MUST support 5 MHz and 10 MHz TDD channels and SHOULD support 3.5 MHz TDD channels in the 1800-1830 MHz band.

9.3 Unlicensed 5.8 GHz Band

The license-exempt frequency band from 5725 MHz to 5875 MHz can be an attractive alternative in regions where the 3650 MHz band is heavily congested. Even with the reduced range due to the higher path losses, solutions in this band can be cost-effective in dense-urban, urban, and some suburban regions. IEEE std 802,16h addresses unlicensed operation.

Therefore;

to enable effective use of the unlicensed 5.8 GHz spectrum allocation it is proposed that the Smart Grid (WiGRID) System Profiles MUST support 5 MHz channel BW in the 5725 to 5875 MHz band and SHOULD support 3.5 MHz channels to facilitate spectrum sharing in congested areas.

9.4 Utility Frequency Band Summary

The following table provides a summary of the proposed channel BWs for the above frequency bands. Channel capacity requirements for Smart Grid M2M applications are comparatively modest. Without specific spectrum allocations for Smart Grid, however, available spectrum will be limited. This will lead to many cases where spectrum will be shared with other operators even in the licensed bands. Smaller channel BWs will facilitate spectrum sharing and interference management with dynamic frequency selection (DFS).

Table 8: Frequency Bands Summary

	Proposed Frequency Bands for WiGRID					
	1.4 GHz		**1.8 GHz**	**2.3 GHz**	**3.65 GHz**	**5.8 GHz**
Channel BW	**FDD** **(A & B)**	**TDD**	**TDD**	**TDD**	**TDD**	**TDD**
3.0 MHz	Should	**Must**		May	May	
3.5 MHz			Should	**Must**		Should
5.0 MHz		Should	**Must**		**Must**	**Must**
7.0 MHz					May	
10.0 MHz			**Must**		**Must**	

Must = Required channel BW
Should = Highly Recommended channel BW
May = Optional channel BW

The relevant OFDM parameters are summarized in the following table along with the UL and DL symbols for a proposed UL to DL ratio of 1.75 to 1 for TDD channels. For this analysis 1 symbol is assumed for the transmit-receive gap which would be typical in most deployments. In rural open areas, 2 or 3 symbols may be necessary for deployments with extended range resulting in a different DL and UL symbol values than those shown in the table.

[9] http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01268.html

Table 9: OFDM Parameters Summary for WiGRID Profiles

Channel BW	**3.00**	**3.50**	**5.00**	**7.00**	**10.00**
Over-Sampling Factor	86/75	8/7	28/25	8/7	28/25
Sampling Frequency	3.44	4.00	5.60	8.00	11.20
FFT Size	**512**	**512**	**512**	**1024**	**1024**
# of Sub-Channels	8	8	8	16	16
Sub-Carrier Frequency Spacing - KHz	6.7188	7.8125	10.9375	7.8125	10.9375
Symbol Time - µsec	148.84	128.00	91.43	128.00	91.43
Guard Time - µsec	18.6	16.0	11.4	16.0	11.4
Symbol Duration - µsec	167.44	144.00	102.86	144.00	102.86
OFDMA Symbols in 5 ms Frame	**29**	**34**	**48**	**34**	**48**
Symbols for TR-Gap	1	1	1	1	1
Data and OH Symbols	28	33	47	33	47
Desired UL/DL Ratio	1.75	1.75	1.75	1.75	1.75
DL Symbols	10	12	17	12	17
UL Symbols	18	21	30	21	30

10. Smart Grid Requirements

The objective of this section is to define the requirements of Smart Grid networks for a new WiMAX Forum system profile.

10.1 Use Cases (Informative)

The maintenance of power transmission lines and generation facilities involves the testing of monitoring and control equipment to verify its operation and connectivity either within the local area and or with the central control system. The Smart Grid functionality serves as a conduit for these activities and communication with the workforce carrying out the maintenance.

The construction of power transmission and generation facilities, in many situations, are in locations poorly served by conventional communications. Wide area wireless communications networks provide communications facilities to manage the construction projects that are often large scale and extend over a considerable period of time that can be years. In addition to the workforce communications, the use of wide area wireless communications networks allows the commissioning of the communications requirements of the facility being constructed.

In the course of the repair of power transmission and generation facilities, Smart Grid communications enabled by wide area wireless communications networks can assist in locating and identifying the repair point and monitoring the progress of such repair to enable outage times to be estimated.

In this section the following use cases are described:

Use Case 1 - Power line and transformer sensors for wide area situational awareness (telemetry).

Use Case 2 - Monitoring the Electrical Distribution System (telemetry).

Use Case 3 - Control of Electrical Distribution Equipment (Distribution Automation).

Use Case 4 - Protection of the Electrical Distribution System.

Use Case 5 - Smart Meter Regional Collectors. (Data Aggregation Points)

Use Case 6 - Remote Site Communications.

Use Case 7 - Direct Meter Reading (AMI)

10.1.1 Use Case – Power line and transformer sensors for wide area situational awareness (telemetry)

10.1.1.1 Description

Power line and transformer sensors are low power devices and may include sensing functionality such as fault indication, voltage, current, line vibration, line temperature, and metering.

Sensors are typically attached to the power system either to a single phase (bird-on-the-wire), to multiple phases, or phase to neutral. When attached to a single phase and inductively powered they have a low power budget and sleep mode become important. Phase to phase and phase to neutral do not have power restrictions.

Power line sensors attached to a single phase and inductively powered are a utility preference due to their ease of installation.

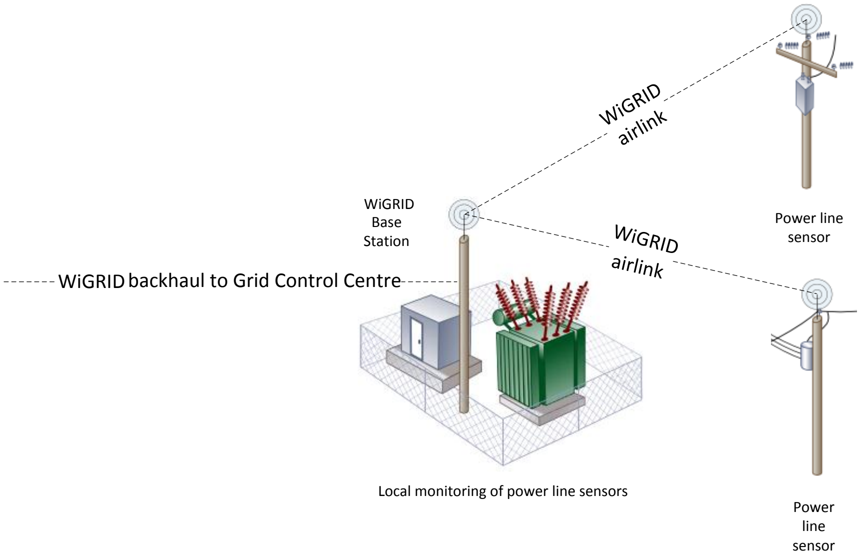


Figure 7 – Wide area situation

10.1.1.2 Actors

Sensor – Power line and transformer sensors

Wide area wireless communications networks Distribution Management System (DMS) – System which consolidates distribution events/status to allow operators like John to manage the electrical network.

10.1.1.3 Pre-conditions

Power line and transformer sensor is attached to a single and multiple phase power transmission line.

10.1.1.4 Post-conditions

Sensor information such as fault indication, voltage, current, line vibration, line temperature, and metering are sent to the DMS.

10.1.1.5 Normal Flow

1. Power line and transformer sensor sends information to DMS over wide area wireless communication networks.
2. To save power, the sensor goes into sleep mode until the next cycle.

10.1.2 Use Case – Monitoring the Electrical Distribution System (Telemetry)

10.1.2.1 Description

This use case is to monitor the Electrical Distribution network and the attached equipment which supports Distribution Automation (DA), Distributed Generation (DG), Fault Management and other system monitoring functions.

Examples of these include:

- Distribution Network Operations: Real-time measurements of Voltage, Power Flows, Harmonics, Phase Unbalance, Power Quality, Switch Status, etc.
- Distributed Generators: Real-time measurements of generation and power quality

- Ancillary Equipment: Real-time status of equipment such as Remote Terminal Units (RTUs) or Intelligent Electronic Devices (IEDs); real-time video feeds (regular or FLIR) from security cameras within a remote station.

The data collected from these devices would be obtained from sensors on the grid, stored, analyzed and presented to operators.

From a network perspective, the requirements for network latency will vary depending on the application. The following are examples:

- **Low Latency**: Required for high priority power systems information (used for real-time decision making in the operations of the electrical network). Examples include SCADA quantities with respect to Power Flows from strategically located devices and/or equipment failure indications.
- **Medium Latency:** Information that could have a large impact on the grid if not monitored as often. Examples of these include DG production, Power Quality.
- **High Latency:** Information that is typically polled once a day to build a system profile over time – these quantities include power quality (such as harmonic distortion) and voltage.

Throughput for this use case also has varying levels. Examples are:

- **Low Bitrate (< 150kbps):** Telemetry data which are less than 100 kbits per transaction, e.g. voltage, power flows, harmonics
- **Medium Bitrate (150 kbps to 300 kbps):** Telemetry data which contains more data points – typically 100-1000 kB per transaction.
- **High Bitrate (>300 kbps):** Real-time Security or FLIR Camera with video feed (HQ streaming at ~700-1000 kbps)

Reliability and availability for these requirements would be dependent on the priority level given to each category.

10.1.2.2 Actors

John – an operator at the grid control center

Electrical Utility – a company which provides electrical transmission/distribution service.

WiGRID Intelligent Electronic Device (IED) – one of the control/telemetry units owned by the Electrical Utility.

Blackbox – securely located in IED.

Grid Control Center (GCC)

Distribution Management System (DMS) – System which consolidates distribution events/status to allow operators like John to manage the electrical network.

10.1.2.3 Pre-conditions

IED has a Blackbox attached. The Blackbox of the IED is equipped with a wide area wireless communications networks module which is certified in the network of the WiGRID Service Provider and interworking with local IED and associated devices. The wide area wireless communications network provides last-mile connectivity from the devices in the field to the DMS at the GCC.

10.1.2.4 Post-conditions

By increasing situational awareness at the grid control center (GCC), this capability is a major contributor to risk mitigation, reliability, outage restoration and customer service. Further, historical data can be accumulated to enhance future forecasting of load requirements.

10.1.2.5 Normal Flow

1. At the GCC, the DMS receives real-time signaling from the IED on a continuous basis over the wide area wireless communications network
2. The information received from the IED, which is monitoring the temperature of a local step-down transformer, indicates that the temperature has been high over the past 24 hours. This is indicative of anoverload condition and/or equipment degradation.
3. Based on the information, John re-routes power flows and prepares a work order to dispatch a field repair crew to identify the cause and take measures for preventative maintenance.

10.1.3 Use Case – Control of Electrical Distribution Equipment (Distribution Automation)

10.1.3.1 Description

The use case is to remotely control the Electrical Distribution network and the attached equipment which supports Distribution Automation (DA), Distributed Generation (DG), Fault Management and other system monitoring functions.

Examples of these include:

- Distribution Network Operations: Planned switching operations on the distribution network.
- Distributed Generators: Planned isolation of Distributed Generators (e.g. during low-demand times)
- Ancillary Equipment: Remote switching and/or configuration at a substation.

From a network perspective, the requirements for network latency will vary depending on the application. The following are examples:

- **Low Latency**: Planned switching events for power systems is work that needs to occur in near real-time.
- **Medium Latency:** Planned switching events which may have a large impact on the grid if not executed in a timely manner. Examples of these include DG production.
- **High Latency:** Planned events which need to be executed but will have minimal system impact if delayed.

Generally speaking, the requirement for this type of remote control requires low throughput since the control signal requires very little data to be transacted.

Reliability and availability of the network for these requirements would be important – more so for high-priority/impact operations.

10.1.3.2 Actors

John – an operator at the grid control center

Electrical Utility – a company which provides electrical transmission/distribution service.

Wide area wireless communications networks.

Switch – one of the IEC61850 control elements owned by the Electrical Utility that allows for remote actuation via a Field Area Network.

Blackbox – securely located in the switch.

Grid Control Centre (GCC)

Distribution Management System (DMS) – System that consolidates distribution events/status to allow operators like John to manage the electrical network.

10.1.3.3 Pre-conditions

Switch has a Blackbox attached. The Blackbox of the Switch is equipped with WiGRID module that is certified in the network of the WiGRID Service Provider. The WiGRID network provides last-mile connectivity from the devices in the field to the DMS at the GCC.

10.1.3.4 Post-conditions

The system correctly performs the required switch operation by remotely actuating Reclosers / Switches within the electrical network. The DMS provides the operator at the GCC a notification that a system switch / reconfiguration has occurred.

1. At the GCC, a scheduled switching event is required.
2. John, via the DMS plans out the appropriate scenario. Upon approval, John executes on the switching plan based on the scenario.
3. The Switch, with a Blackbox attached, receives real-time signaling from WiGRID network to perform a switch operation (i.e. open).
4. The remote switch operation is completed and a confirmation message is sent via the Blackbox and the attached WiGRID network to the DMS.
5. John receives the notification and confirms that the operation has concluded.

10.1.4 Use Case – Protection of the Electrical Distribution System

10.1.4.1 Description

The requirement identified in this use case; is to monitor and ensure power system protection with the presence of DA-enabled devices through optimized group relay settings which can be changed automatically and remotely.

The purpose of this is to allow for protection (i.e. electrical isolation of elements from harm after a local event) and control (i.e. remote reconfiguration of the distribution network to bypass isolated element) to increase the reliability and resiliency of local electricity service.

The protocol used in this use case is the IEC 61850 Generic Object-Oriented Substation Event (GOOSE) message. This is the enabling network layer protocol between power systems devices.

From a wide area wireless communications networks network perspective, there is a requirement for **low network latency** in the neighborhood of **20-30 ms** per network hop for the transit time across the network communications medium due to the timing sensitivity around the isolation of electrical equipment.

Throughput for this use case will be **low (< 150 kbps)**.

Within this use case, reliability and availability are paramount as a network event can occur at any given moment and the system needs to be able to react quickly (i.e. overall response time¸ including power systems equipment, needs to occur within 500-700 ms).

10.1.4.2 Actors

John – an operator at the grid control center

Recloser / Switch – one IEC61850 enabled device, owned by the Electrical Utility and installed on its electrical distribution infrastructure, which is capable of opening/closing remotely to enable connectivity/disconnection of the distribution power line.

Blackbox – securely located in the Recloser / Switch.

Controller – IEC61850 enabled controller unit which resides at a central location.

Grid Control Centre (GCC)

Distribution Management System (DMS) – System which consolidates distribution events/status to allow operators like John to manage to the electrical network.

10.1.4.3 Pre-conditions

Recloser / Switch has a Blackbox attached. The Blackbox is equipped with a WiGRID module which is certified in the network of wide area wireless communications networks. The wide area wireless communications network provides last-mile connectivity from the devices in the field to the DMS at the GCC.

10.1.4.4 Post-conditions

In the event of a fault, the system correctly and automatically isolates the section via remotely actuating Reclosers / Switches within the electrical network. The DMS provides the operator of the GCC a notification that a system event has occurred and the local electrical distribution network has been reconfigured.

10.1.4.5 Normal Flow

1. A fault-to-ground event occurs in the field on a section which contains Recloser /Switches that are IEC61850 and wide area wireless communications network enabled.
2. This event is sensed by the Recloser / Switch within the local electrical distribution network segments. By utilizing the IEC61850 GOOSE protocol, the local Recloser / Switch sends a message upstream using the attached Blackbox over the WiGRID module, to the local IEC61850-enabled controller unit.
3. The local IEC61850 controller unit processes the information received and executes one of the pre-mapped scenarios to isolate the local electrical distribution line segments by sending remote commands downstream to the affected Reclosers / Switches to open or remain closed.
4. The affected Reclosers / Switches receive the GOOSE message from the controller unit and performs its switching operation. A confirmation message is returned to the local controller unit .
5. The DMS receives the information from the local controller that a fault-to-ground event has occurred and that a switch operation has taken place.
6. John verifies that the network has been correctly reconfigured and prepares a work order to dispatch a field repair crew to identify the source of the fault-to-ground event and take the necessary steps to repair it.

10.1.5 Use Case– Smart Meter Regional Collectors

10.1.5.1 Description

The requirement is to connect Smart Meter Regional Collectors (RCs) or Data Aggregation Points (DAPs) to the Smart Meter head-end server (HES) using wide area wireless communications network, in order to aggregate information from Smart Meters located at the customer's premise.

There are 3 general scenarios:

1. Scheduled polling of interval data – Hourly interval usage data is polled from the RC or DAP. These are regularly scheduled communications between the RCs and the HES and the average bit rate per transaction is roughly 20 kb/s with peaks of 64 kb/s.
2. On-demand polling – To perform a real time transaction from the HES to a specific meter (through the RC) to obtain Time-of-Use electricity usage information. The individual transactions are typically very small (i.e. <50 kb of information transacted) but it is dependent on how many users attempt to perform these transactions.

3. Event Notification from the field – Smart Meters are equipped with power-outage notification capability which will use the network to initiate communications back to the HES to notify the system operators of any power outages in the field. The individual transactions are typically very small (i.e. <10 kb of information transacted to notify the HES) but may originate from a large number of end points (e.g. local power outage affecting several hundred homes will result is several hundred events generated in a short period of time).

Through consistent polling of the Smart Metering network, The Electric Utility can monitor short and long term trends in its customer's consumption and take corrective action in advance.

The Electric Utility can monitor the smart meters for any disruption, caused by events and dispatch a field repair crew to identify the cause and take measures to restore the service more effectively.

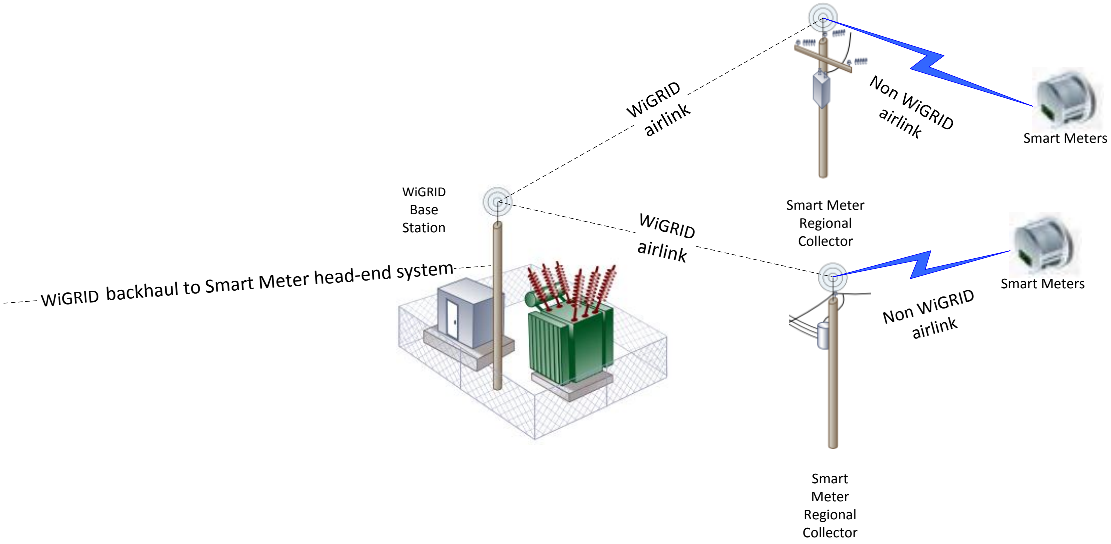


Figure 8 – Regional collectors

10.1.5.2 Actors

Mike – a Smart Meter Network Operator (SMNO) at the utility

Wide area wireless communications network Smart Meter Regional Collectors – a device that collects information from Smart Meters that are located at utility customer locations and transfers the information to the Smart Meter head end.

Smart Meter Head-End Server – a server located in a utility company premise.

Smart Meter – a device that monitors electricity consumption at a utility customer location.

10.1.5.3 Pre-conditions

The Smart Meter Regional Collector is installed and configured to connect to the Smart Meter Head-End Server located in the utility data center. The Smart Meter Regional Collector is equipped with a WiGRID module that is both within the coverage area and certified in wide area wireless communications networks. The Smart Meter Regional Collector connects to smart meters in its designated area.

10.1.5.4 Post-conditions

The Smart Meter Regional Collector provides metering information to the Smart Meter Head-End Server and Mike can see the retrieved information from at the Smart Metering Head-End Server (HES).

10.1.5.5 Normal Flow

1. The HES is scheduled and configured to poll the RC twice a day to obtain interval reads from Smart Meters downstream of the RC.
2. A polling request is initiated at the HES through the WiGRID-enabled network to the remotely installed RC.
3. The poll executes successfully and electrical consumption information from Smart Meters located at customer locations covered by the RC is successfully downloaded.

10.1.5.6 Alternative Flow

Event notification from the Smart Meters in the field may be sent through the RC to the HES using the WiGRID network.

10.1.6 Use Case – Remote Site Communications

10.1.6.1 Description

Providing communications to under serviced utility premises for Corporate WAN connectivity for permanent and temporary sites, such as remote offices, substations, and construction sites.

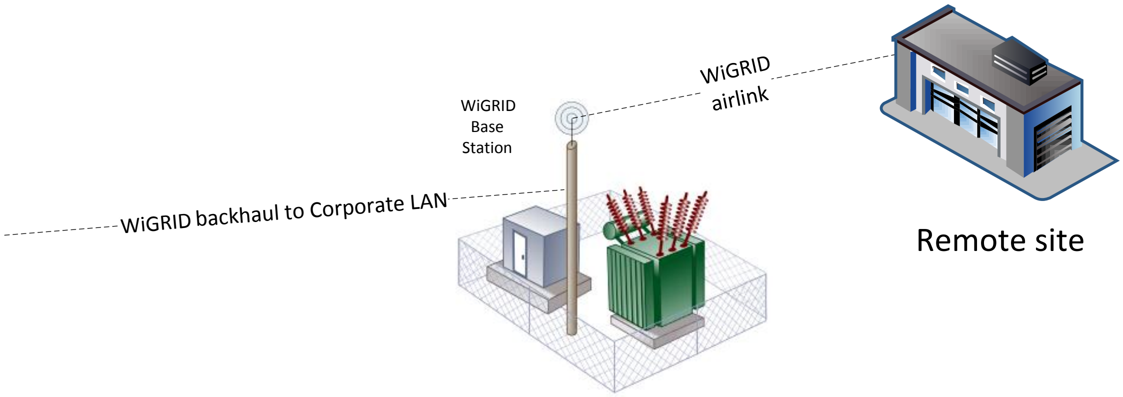


Figure 9 – Remote site communications

10.1.6.2 Actors

Paul – an operator at the Electrical Utility

John – an operator at the Remote Site

Electrical Utility – a company which provides electrical transmission/distribution service.

Wide area wireless communications network Underserved Utility site – A permanent or temporary utility site.

Site LAN switch – A LAN switch located at the permanent or temporary site.

10.1.6.3 Pre-conditions

The Site LAN router/switch is located at the Underserved Utility site and is connected to a WiGRID® CPE device that is certified in the network of the WiGRID Service Provider. The Site LAN router/switch is connected to a number of site end devices such as wireless routers, PCs, servers, and/or VoIP switches.

10.1.6.4 Post-conditions

The Site LAN switch provides either permanent or temporary secure access to corporate WAN facilities.

10.1.6.5 Normal Flow

1. At the permanent or temporary underserved site, John can access email.
2. At the permanent or temporary underserved site, John can use VoIP facilities.
3. At the permanent or temporary underserved site, John can both download and upload data to corporate data bases.

10.1.7 Use Case– Smart Meters: Direct Meter Reading and HAN Services

10.1.7.1 Description

The requirement is to connect Smart Meters, that have an integrated 4G communications module to Smart Meter head-end server (HES) using a wide area wireless communications networks, in order to;

- Deliver information, primarily meter readings, from Smart Meters located at the customer's premise
- Update meter firmware to add new metering applications
- Communicate with Appliances at the customer premises via the Home Area Network (HAN)

There are the following general usage scenarios:

1. Scheduled polling of interval data – Minute or Hourly interval usage data is polled from the RC. These are regularly scheduled communications between the RCs and the HES and the average bit rate per transaction is roughly 1 kb/s with peaks of 5 kb/s.
2. On-demand polling – To perform a real time transaction from the HES to a specific meter (through the RC) to obtain Time-of-Use electricity usage information. The individual transactions are typically very small (i.e. 1500 bytes of information transacted).
3. Event Notification from the field – Smart Meters are equipped with power-outage notification capability (Last-Gasp transmissions) which will use the network to initiate communications back to the HES to notify the system operators of any power outages in the field. The individual transactions are typically very small (i.e. 1500 bytes of information transacted to notify the HES) but may originate from a large number of end points (e.g. local power outage affecting several hundred homes will result is several hundred events generated in a short period of time).
4. Firmware Updates to the Meter and 4G Communications modules – During the operational life of the Smart Meter, the 4G communications module (which may include a ZigBee radio) will need updating. A typical firmware update is approximately 1 Mbyte.
5. Real-time messaging to / from the Home Area Network – The 4G communication module can act as a communication gateway for a ZigBee or HomePlug Home Area Network. This allows the Utility to send and receive messages from Smart Appliances within the Consumer's premises.

A 4G Smart Metering network allows the Electric Utility to monitor short and long term trends in its customer's consumption and take corrective action in advance.

The Electric Utility can monitor the smart meters for any disruption, caused by events and dispatch a field repair crew to identify the cause and take measures to restore the service more effectively.

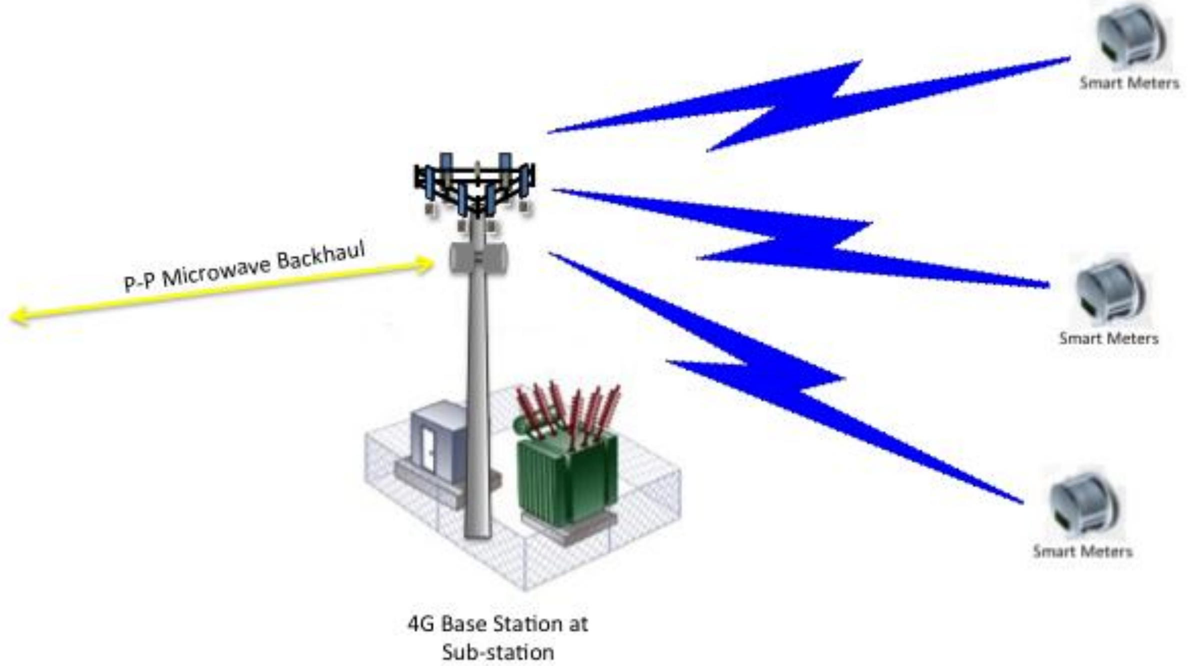


Figure 10 – Direct Meter Reading

10.1.7.2 Actors

Mike – a Smart Meter Network Operator (SMNO) at the utility.

Smart Metering WiMAX/4G Network, capable of supporting large numbers of meters.

4G Smart Meter – Smart Meters that have integrated 4G communication modules that collect consumer metering data and act as a communications gateway to the HAN.

Smart Meter Head-End Server – a server located in a utility company premise.

10.1.7.3 Pre-conditions

The Smart Metering WiMAX/4G Network is installed so that it provide coverage to the target service area which will contain the Smart Meters. The Smart Metering WiMAX/4G Network is connected to the Smart Meter Head-End Server located in the utility data centre. Typically there is a WiMAX Core Network responsible for managing the Smart Meter WiMAX/4G networks. This core network contains an ASN-GW and AAA Server.

10.1.7.4 Post-conditions

The Smart Meter WiMAX/4G Networks passes metering information to and from the Smart Meter Head-End Server and Mike can see the retrieved information at the Smart Metering Head-End Server (HES).

10.1.7.5 Normal Flow

1. The HES is scheduled and configured to poll the RC twice a day to obtain interval reads from Smart Meters downstream of the RC.
2. A polling request is initiated at the HES through the WiMAX/4G-enabled network to the remotely installed RC.

3. The poll executes successfully and electrical consumption information from Smart Meters located at customer locations covered by the RC is successfully downloaded.

10.1.7.6 Alternative Flow

Event notification from the Smart Meters in the field may be sent through the RC to the HES using the WiMAX/4G network.

11. IEEE 802.16 Requirements (Conditional Normative)

11.1 Service Requirements

11.2 Functional Requirements

11.2.1 System Requirements

The following system requirements are divided into two groups. The first group defines system requirements for "WiGRID-1. The system requirements for WiGRID-1 are based on features included in IEEE Std 802.16e-2009 [6] (or optionally in IEEE Std 802.16m [7]). The second group defines an advanced set of system requirements for "WiGRID-2". This set of requirements draws on features being developed for 802.16n [8] and 802.16p [9]. It is mandatory for WiGRID-2 to be backwards compatible with WiGRID-1.

Since the 802.16n [8] and 806.16p [9] amendments have not yet been completed and ratified, the WF SGWG feels that a two-phase approach is more expedient for developing system profiles for WiGRID that specifically address key requirements for Smart Grid networks to ensure timely commercial product availability. It is anticipated that WiGRID-2 would trail WiGRID-1 by 12 to 18 months.

The functional requirements for WiMAX-2 defined in this version of the WiMAX Forum System Requirements Specification should be considered preliminary. These will be updated as work on 802.16n [8] and 802.16p [9] is completed. Further updates to the functional requirements for WiGRID-2 may also prove necessary to meet Smart Grid requirements being developed by the SGIP and OpenSG Users Group.

11.2.2 WiGRID-1 System Requirements

Layer 2 Support: Most Field Area Network applications are fixed not mobile and support for mobile IP is not necessary or helpful. Most networks operate at Layer 2 and therefore all WiGRID devices shall support the Ethernet convergence sub-layer, rather than the IP Convergence sub-layer. Support for ETH-CS should still enable the use of packet classification and other features used to drive QoS and VLAN operation.

Optimized Latency: Need to have optimized support for utility-specific applications such as IEC61850 GOOSE multicast messaging (Layer 2 multicast support). It is anticipate that the UGS service flow will need to be slightly modified to allow the latency/QoS objectives of the protocol to be met (i.e. ensuring the 155 byte GOOSE multicast frame is not segmented across multiple WiGRID frames thereby causing increased latency). In particular, low layer 2 latency in the order of magnitude of 15-30 ms per hop, is required to support GOOSE. Whether or not GOOSE is used, this is still relevant in power systems applications (e.g. mirrored bits).

When used for stationary devices, (e.g. for Smart Grid applications) the WiGRID Network SHALL support message delivery reliability of at least 99.5 % with latency not to exceed 100 ms, 99.7 % with latency of 200 ms, and 99.8 % with latency of 400 ms.

These requirements apply to not more than 2 hops, in an operationally loaded network. The latency does not include any time required for the repair in case of a degraded network. (per 802.16p [9]).

WiGRID interoperability assumes a minimum latency in loaded and non-loaded conditions between the Base Station and the Subscriber Station.

Number of Active Terminals (Actors): For WiGRID to be considered for direct connection to smart meters, as in an AMI network, it must have the ability to simultaneously handle traffic from a large number of terminals or end-points. Average packet sizes will be small but the number of terminals (actors) per base station can exceed several thousand in a dense urban environment. Additionally, in the absence of dedicated spectrum, channel BWs may be limited. As WiGRID is deployed upstream from the AMI network, total data requirements will be comparable but the number of active terminals per channel will be significantly less but with larger average packet sizes.

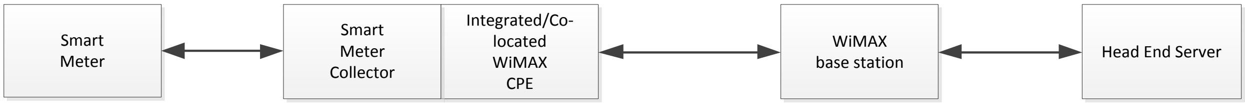
The number of active terminals per sector in a WiGRID AMI network will exceed 1800 terminals (meters) in a dense urban area of >4000 HU per sq-mi assuming a 3-sector BS coverage area of 0.66 sq-mi (1.7 sq-km). The following requirement will enable a WiGRID 3-sector base station in an AMI network to support more than 5000 smart meters with a 3.5 MHz TDD channel BW and a UL to DL ratio or at least 1.75.

A Channel SHALL support >1000 Active Terminals per MHz and SHOULD support >1500 Active Terminals per MHz under the following conditions: Average payload = 350 Bytes, Latency < 1 Second at the application layer with 99.5% confidence.

Extended Operating Reach: Network operating reach on a single PtP link SHALL be at least 37 km and SHOULD permit a range up to 52.5 km (with an appropriate channel bandwidth and EIRP).

Interoperability: Interoperability SHALL be supported if the same device types are used; the WiMAX Forum SHALL facilitate interoperability testing and certification amongst vendors of WiGRID devices.

UL and DL traffic for Smart Grid Networks: The communication requirements for Smart Metering and Smart Grid applications are well suited to point to multipoint technologies such as WiGRID. For Smart Metering, the meter is typically connected to a smart meter collector (aka DAP or RC) that is backhauled using WiGRID from either an integrated or collocated WiGRID CPE to the base station and then on to the HES



Although the data center sends requests to read the smart meter information, to which the meter or meters respond back to the data center, the data throughput direction is generally biased towards the uplink.

In the case of Smart Grid applications, the IEDs either respond to requests from a central location or respond based on the occurrence of an event to the central location.

These two instances outline the uplink bias of the data flow, whereas the existing WiMAX system profiles have centered around having the data flow biased in the downlink to meet their market requirements. To readdress this and increase the UL capacity, a number of options are available for WiGRID profiles,

a) Increasing the output power of the CPE to enable the highest UL MCS to be used.

b) Changing the DL to UL ratio, such that the UL time is greater than the DL, this is similar to increasing the output power, since the CPE is transmitting for a longer period.

c) CPE support for multiple transmit antennas and Spatial Multiplexing (Matrix B) in the UL for added UL capacity and support for Transmit Diversity (Matrix A) for increased UL system gain. Since the UL link budget is generally the limiting factor for coverage Increased UL system gain will translate to increased coverage or an increase in UL availability.

Regarding option a) and c), although having a larger output power could increase the channel capacity, it has been shown to be more efficient to have more than one lower power transmitter as opposed to one large transmitter[10] . It is therefore proposed that a CPE supporting UL MIMO is desirable in Smart Metering and Smart Grid applications. Changing the DL to UL ratio to increase the throughput is complimentary to UL MIMO as a means for increasing the uplink capacity.

The following 4 requirements address the need for enhanced UL data capacity.

UL/DL Ratios: In a Smart Grid network, as stated above, UL traffic will dominate a majority of the time, exceptions to this will occur when SW upgrades are being downloaded to terminal devices. Being able to adapt TDD profiles to favor either UL or DL will be an important WiGRID feature for Smart Grid applications.

TDD Profiles SHALL support adaptive DL/UL ratios from 1.75:1 to 1:1.75***UL Modulation:*** In addition to data dominating the UL traffic, it will be necessary to support video streaming in the UL for surveillance and disaster recovery.

[10] http://www.sequans.com/pdf/SequansUplinkMIMOWP0608_v2.pdf

UL 64QAM with 5/6 coding SHALL be supported

UL Permutation: To reduce UL channel OH, AMC SHALL be supported in the UL Note: Sacrificing mobility capability is acceptable for Smart Grid applications which are predominately fixed or nomadic.

MIMO: MIMO (Matrix A/B), transmit diversity and spatial diversity SHALL be supported in the DL and UL and MU-MIMO SHALL be supported in the UL.

Terminals/CPEs SHALL support (2x2) MIMO with Tx power up to 30 dBm (which is permitted in most deployment scenarios).

QoS: Establish QoS Profiles that are optimized for power system applications (i.e. with latency enhancements as stated above – maybe a subset of UGS).

The WiGRID SG Network SHALL provide MAC enhancements to support high reliability latency intolerant control and reporting messaging.

The WiGRID MAC SHALL be able to support priority access services for ETS (Emergency Telecommunications Services) and other priority and latency-sensitive applications.

Security procedures for WiGRID SG-Network

WiMAX SG Network SHALL support secure communication and session establishment among Terminals, and between Base Stations and external AAA-servers**.**

ASN Profile: An optimized ASN is required to support high reliability, handover in a fixed environment. Need to apply various models with respect to ASN's – Profile A or B or in standalone mode with no ASN.

Nomadic Application: A subset of the utility radio access network involves a Nomadic application (semi-transportable remote radio) for field crews and increase overall network reliability; work is required to develop how traffic is handled when CPE's are moved from various base stations and their associated L2 domains.

Base Station Relay/Multi-Hop Support: The WiMAX network SHALL support BS to BS connectivity in support of relaying functionality.

WiGRID Smart Grid Base Station: SHALL support both ETH-CS and "ASN-GW-Less" Operation, i.e. Edge Router functionality in Base Station.

11.2.3 WiGRID-2 System Requirements

The IEEE 802.16n amendment [8] (aka GRIDMAN) is designed to develop features and attributes leading to higher system and network reliability and robustness consistent with utility requirements for Smart Grid networks. The IEEE 802.16p amendment [9] is focused on Machine-to-Machine (M2M) interfaces. In this context enhanced features are developed for: reduced power consumption, lower OH for large numbers of users with small burst (packet) sizes, and enhanced security measures. The following system requirements for WiGRID-2 are preliminary and will be updated when IEEE Std 802.16n [8] and 802.16p [9] are ratified and the SGWG has had ample opportunity to completely review the new features and evaluate their applicability for WiGRID-2. From what is known so far, the following are considered important for inclusion in WiGRID-2. In reviewing the preliminary requirements for WiGRID-2 and considering the status of the 802.16 amendments, the WF-TWG is encouraged to include any of the following features in the WiGRID-1 profiles.

Security Requirements: The WiGRID SG Network topology SHALL not degrade the security performance achieved with WirelessMAN OFDMA or WirelessMAN-Advanced Air Interface in hierarchical network topology.

Network aided mutual authentication of Terminals and data security

Terminals SHALL be able to establish a security association with each other. A security server may be used to facilitate the establishment of security associations.

Autonomous (limited) mutual authentication of HR-MS and data security for direct communication

Terminals SHALL be able to mutually authenticate themselves without access to a security server.

Terminals SHALL be able to establish encrypted communication without access to a security server.

Security requirements for HR-Network nodes acting as relays

Base Stations that functions as a relay SHALL forward security related messages between other Base Stations and a security server, both during security association establishment and ongoing communications.

Multicast key Management

WiGRID SG-Network SHALL provide the security architecture that provides a group of Terminals with authentication, authorization, encryption and integrity protection.

WiGRID SG Network SHALL provide multicast key management for groups of Terminals. The key shared within the group SHOULD be distributed securely and efficiently. WiGRID SG Network SHOULD support the group signaling procedure using multicast transmission for multicast key management efficiency.

(above security requirements per 802.16n [8])

Network Diversity/Resiliency Support: WiGRID SG network SHALL be able to recover from any Single-Point-of-Failure (SPoF) of any of its infrastructure nodes (e.g. excludes terminal/subscriber station nodes) per 802.16n [8].

Network SHALL provide local connectivity to terminals within the Base Station coverage area in the absence of BS connectivity to the backbone network. i.e when the BS loses the backbone connection the established service flow between terminals within the coverage area of the BS SHALL be maintained. (per 802.16n [8])

Terminal to Terminal Connectivity (single-hop): Terminal SHALL support communication of user data and control signaling between a Terminal and one or more Terminals that are 1-hop away. (per 802.16p [9])

Terminal to Terminal Connectivity (two-hop): Terminal SHOULD support forwarding of user data and control signaling between a Terminal and one or more Terminals that are two hops away. (per 802.16p [9] SHALL)

Terminal Forwarding to Network: Terminal forwarding is defined as the case where the origination and termination of data are at the Terminal and network respectively and vice versa.

WiGRID SG Network SHALL support Terminal forwarding of user data and control signaling between Terminal and Base Station and between Terminal and Relay Station. The control signaling and data transmission for the Terminal to Terminal direct link SHALL at least be capable of operating within the frequency band that the Base Station operates.

An association establishment SHALL be supported. (per 802.16n [8]).

Path Discovery: WiGRID SG Network SHALL support neighbor and path discovery between Terminals as well as between Terminal and Network infrastructure stations. Path discovery can be accomplished with or without network support. (per 802.16n).

Path Management: WiGRID SG Network SHALL support establishment and maintenance of alternative paths to support fast recovery in the event of disruption; for example, encountering intermediate Terminal failure or movement. WiGRID SG Network SHALL support the capability to choose the most reliable path. (per 802.16n [8]).

Local Forwarding for Relay Station and Base Station: WiGRID SG Network SHOULD allow local forwarding, which allows one Terminal to communicate to one or more Terminals via infrastructure station without going through the backhaul (per 802.16n [8]).

Unicast and Multicast Enhancements: WiGRID network SHALL provide optimized MAC protocols for enhanced unicast and multicast transmission to support two-way communications such as Push to Talk (PTT) service among a group of Terminals Examples of applications to be used in PTT service include:

- audio (speech)
- video
- still image
- text (formatted and non-formatted)
- file transfer

11.2.4 Network Requirements

11.2.4.1 Network Management Requirements

With the increased number of smart grid field devices requiring remote management, the WiGRID smart grid network will also need to provide a suite of standard protocols and functionality to support monitoring, management, and incident resolution with the WiGRID network.

General Network Management Requirements

1. Lightweight management protocols MUST be used to minimize performance degradation and overhead.
2. Network elements MUST support, at a minimum, the following network management functions:
    a. Fault data – identification and analysis of incident alerts (e.g. ASN-GW server down alert) to send to an element manager.
    b. Performance data – collection and calculation of real-time and historical data (e.g. current link latency) to sent to an element manger.
    c. Configuration Management – remote configuration and management (e.g. remote subscriber station firmware update) via command line or element manager pass through.
3. Management functionality MUST extend to the subscriber station.
4. Network elements MUST provide information about their location in the network topology.
5. Open northbound interface support either through standardized protocols (e.g. SNMP) or easily interpretable file structures (XML) MUST be available.
6. Network management protocols MUST provide authentication between network elements and element management systems.
7. Network management protocols MUST encrypt management information between network elements and element management systems.
8. Equipment identification information MUST be collected remotely from the network elements and should include:
    a. Hostname
    b. IP address
    c. Software / firmware version
    d. Location description
    e. Serial number

Fault Management Requirements

1. Network elements MUST be configurable to send incident alerts to 2 or more 3rd party management systems.
2. Incidents alerts MUST contain detailed messaging that can be interrupted by the element management system to perform root-cause analysis and should include:
    a. Hostname
    b. IP address
    c. Equipment location
    d. Incident severity indicator
    e. Incident type

f. Incident description

3. SNMP MUST be used, at a minimum, for incident alerting. Advanced notification interfaces (e.g. vendor specific APIs) should only be used if they are thoroughly documents and interoperable with common OSS platforms.
4. Open MIB files MUST be used for SNMP traps.

Performance Management Requirements

1. Near real-time performance data MUST be available from the network element.
2. Performance data MUST be available via an open protocol such as SNMP or xml to be interpreted by the element management system.
3. Network elements MUST be configurable to send performance data to 2 or more 3rd party systems.
4. Performance data collected and sent to the element management system MUST include:
   a. Network element uptime
   b. Network interfaces
   c. Interface throughput
   d. RSSI (base stations and subscriber stations)
   e. Link health
   f. Processor health
   g. Memory used vs. free

Configuration Management Requirements

1. Network elements MUST support remote configuration using secure protocols such as SSH and HTTPs.
2. Network element provisioning and configuration MUST be available remotely.
3. Network elements MUST provide remote firmware update capabilities.

11.2.5 Air Interface Requirements

11.2.6 Security Requirements

11.2.6.1 Privacy Requirements

11.2.7 Policy Control & QoS Requirements

11.2.8 Regulatory Requirements

Regulatory requirements must always be considered in accordance with the applicable national/regional laws and technical regulations.

12. System Analysis: Impact of Proposed New Features

In considering system profiles that are more optimally suited for Smart Grid networks a number of new features were proposed for WiGRID in Section 10. Among these were several features that addressed the significantly different traffic patterns that can be expected in a Smart Grid network, as compared to traditional broadband mobile networks. Mobility is another WiMAX feature that is less important in Smart Grid networks, with that understanding, AMC permutation can be considered to be ‘standard” for WiGRID profiles.

In this section we show how the WiGRID features translate to key deployment metrics leading to a more optimized and more cost-effective WiMAX solution for Smart Grid networks. The following system analyses illustrate the deployment benefits for both a range-constrained deployment (section 12.2) and a capacity-constrained deployment (section 12.3).

This system analysis is based on Utility Requirements outlined in section 10 of this document. Specific bit rate estimates for UL and DL message traffic is provided in the following table in Section 12.1.

12.1 Use Case Communications Requirements

Table 10: Use Case Communications Requirements

Use Case	DL (kbit/s)	UL (kbit/s)	Latency (ms)	Packets per Sec	Msg. Freq.	Payload Type	Active / Idle	Predictability
1 - Situational Awareness	1.0 kbit/s	5.0 kbit/s	1000 ms	5 pps	5 sec	TCP	1sec / 5sec	Good
2 - Monitoring	~10 kbit/s	~300 kbit/s	100 ms	100 pps	100 ms	TCP and UDP	Active	Good
3 - Control	1.0 kbit/s	5.0 kbit/s	100 ms	10 pps	1 sec	TCP	1sec / 5sec	Random
4 - Protection	150 kbit/s	150 kbit/s	20 ms	100 pps	100 ms	UDP	Active	Random
5 - Metering Regional Collector	5 kbit/s	64 kbit/s	1000 ms	20 pps	100 ms	TCP	Active	Good
6 - Remote Site Communications	500 kbit/s	500 kbit/s	100 ms	100 pps	20 ms	TCP	Active	Good
7 - Direct Smart Meter Reading (AMI)	0.05 kbit/s	1.0 kbit/s	5000 ms	1 pps	5 min to 6hr	TCP	100ms / 4secs	Good

12.2 Range-Constrained Deployment with Baseline “WiGRID-1” System Profile

- Baseline (WiGRID-1): “standard” 802.16e (Not Open Retail)
- Add 64QAM 5/6 in UL
- Add Uplink Centric Frame Splits

  Up to 14:33 (in 5 or 10 MHz channels)
- Add Uplink CSM and/or Uplink Matrix B MIMO
- Add Uplink Band-AMC Support
- Add ETH-CS and “ASN-GW-Less” Operation

  Edge Router functionality in Base Station

  Layer 2 operation
- Add Range Extension

  Up to 37 km Increased TTG (1 or 2 Blank Symbols)
- Add support for High Power CPEs

  Up to 2 x 30 dBm

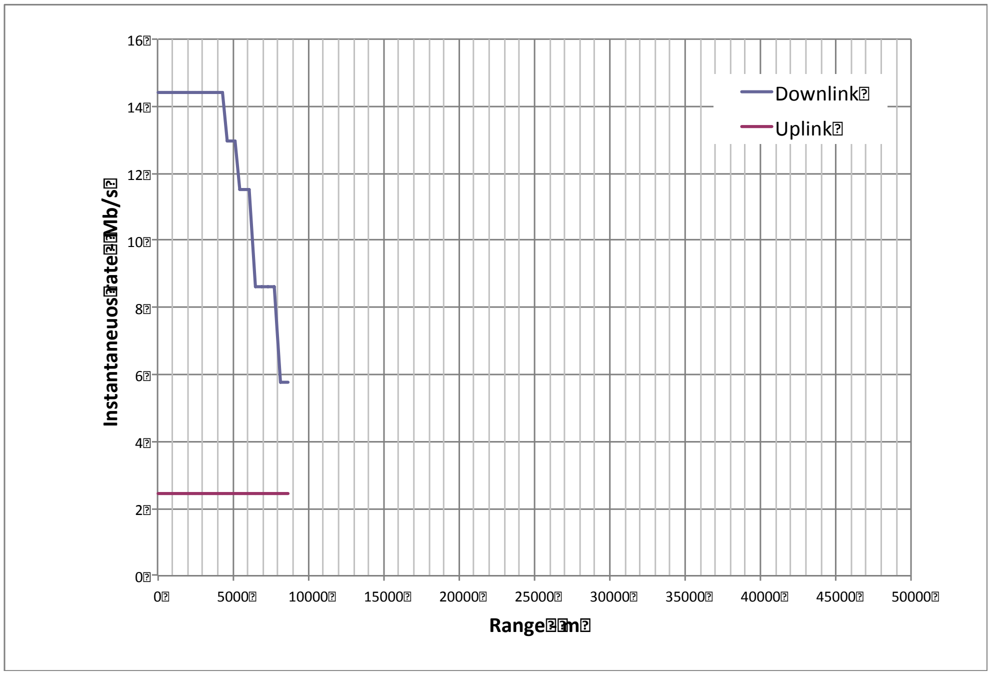
12.2.1 Standard 802.16e System Profile

Range Vs. Throughput

Profile Assumptions:

- 1800 MHz / SUI-C
- 5 MHz Channel
- Non-Segmented
- BS=40m, MS=5m
- Standard CPE
  - ○ 27dBm and 1Tx
- 26:21 Frame Split
- Standard Range
  - ○ 8.3km Limit
- UL 16QAM
- IP-CS (w/MAC OH)

Max rates	
DL	14.4
UL	2.45
Total	16.85



DL Centric, Range limited by TTG, Uplink Capacity = 14.5%, Channel = 16.9 Mbit/s

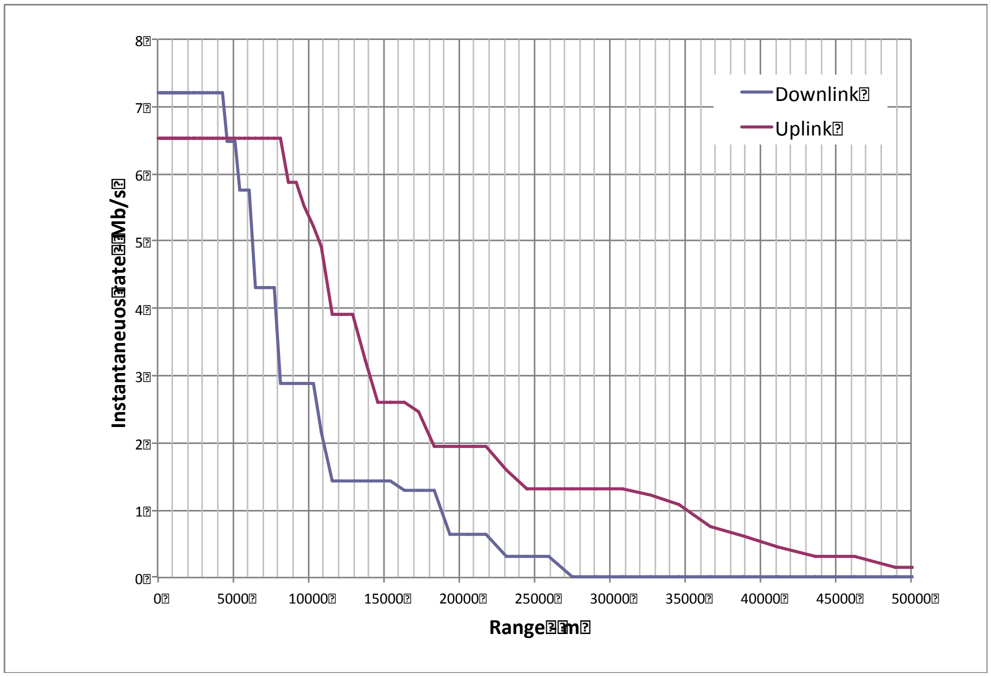
12.2.2 WiGRID-1 System Profile

Range Vs. Throughput

Profile Assumptions:

- 1800 MHz / SUI-C
- 5 MHz Channel
- Non-Segmented
- BS=40 m, MS=5 m
- Standard CPE
    - ○ 27dBm and 1Tx
- 17:30 Frame Split
- Long Range (2 SYM)
    - ○ 37 km
- UL 64QAM
- ETH-CS (w/MAC OH)

Max rates	
DL	7.2
UL	6.53
Total	13.73



Symmetric, Range extended to 37 km, Uplink Capacity = 47%, Channel = 13.7 Mbit/s

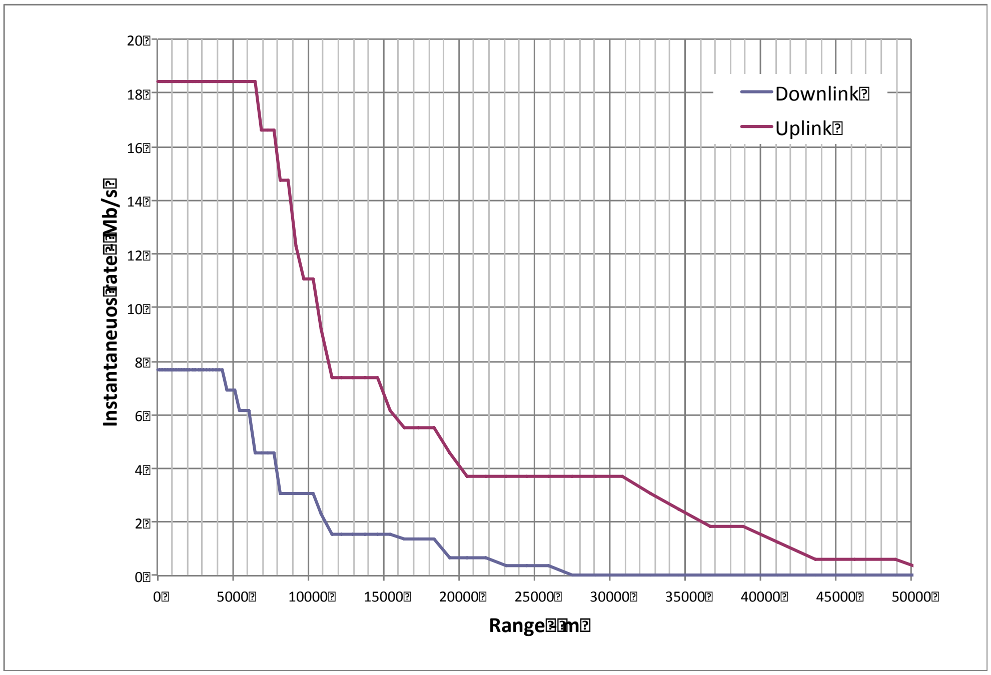
12.2.3 WiGRID-2 System Profile

Range Vs. Throughput

Profile Assumptions:

- 1800 MHz / SUI-C
- 5 MHz Channel
- Non-Segmented
- BS=40 m, MS=5 m
- High Power CPE
- 17:30 Frame Split
- Long Range (2 SYM)
    - 37 km
- UL CSM / Matrix B
- UL 64QAM
- UL Band-AMC
- ETH-CS (w/MAC O/H)

Max rates	
DL	7.68
UL	18.43
Total	26.11



Uplink Centric, Range = 37 km, Uplink Capacity = 70%, Channel = 26.1 Mbit/s

12.2.4 Comparison

Table 11: Band Width Comparison

5 MHz @ 1800 MHz	Standard 16e WiMAX	Basic 16e WiGRID-1	Advanced 16e WiGRID-2
Peak DL	14.4 Mbit/s	7.2 Mbit/s	7.7 Mbit/s
Peal UL	2.5 Mbit/s	6.5 Mbit/s	18.4 Mbit/s
Peak Total	16.6 Mbit/s	13.7 Mbit/s	26.1 Mbit/s
8km			
Average DL	6.0 Mbit/s	2.9 Mbit/s	2.9 Mbit/s
Average UL	2.5 Mbit/s	6.5 Mbit/s	14.8 Mbit/s
Average Total	8.5 Mbit/s	9.4 Mbit/s	17.7 Mbit/s
25km			
Cell Edge DL	-	0.35 Mbit/s	0.35 Mbit/s
Cell Edge UL	-	1.3 Mbit/s	3.7 Mbit/s
Cell Edge Total	-	1.65 Mbit/s	4.1 Mbit/s

12.2.5 Conclusions: WiGRID Profile

"Standard" 802.16e [6] WiMAX profiles are not optimal for Utility Applications.

Symmetric and Uplink-centric applications limited to reduced ranges and lower data rate.

- WiGRID-1 profile extends operational range (up to 37 km) and supports symmetric and uplink centric application at higher channel data rates.
- WiGRID-2 profile can deliver large spectral efficiency gains, and massive uplink capacity improves at long operational ranges.

12.2.6 Multi-Use Utility Network

Table 12: Example Scenario

Multi Use Network	DL (kbit/s)	UL (kbit/s)	Qty	Total DL (kbit/s)	Total UL (kbit/s)
1 - Situational Awareness (WASA)	1	5	5	5	25
2 - Monitoring	10	300	10	100	3000
3 - Control	1	5	5	5	25
4 - Protection	150	150	5	750	750
5 – Metering Regional Collector (RC or DAP)	5	64	10	50	640
6 – Remote Site Communications	500	500	3	1500	1500
7 – Direct 4G Smart Metering (AMI)	0.05	1	100	5	100
Total				2415	6040

Standard 802.16e = 3 Radios

WiGRID-1 = 1 Radio (93% Loaded on Uplink)

WiGRID-2 = 1 Radio (40% Loaded on Uplink)

12.3 Capacity-Limited Scenario for a Dense Urban Area

The above analysis illustrates the benefits achieved with features designed to enhance UL channel capacity in a range-limited deployment scenario. It is also important to understand the benefits and relative cost saving, measured by base station requirements that will be realized in a capacity-limited scenario typically encountered in a dense urban or urban environment.

Dense urban has been defined by the OpenSG-Network/Communications Working Group as areas having a Housing Unit (HU) density higher than 4000 HU/sq-mi.(1545 HU/sq-km) In the United States, 11% of the population live in Dense Urban areas meeting this density criteria. Accounting for electric, water, and gas meters plus feeder circuits etc and enterprise customers, the density of SG actors will exceed 10,000/sq-mi. Under most conditions wireless deployments and the number of base stations required in these areas will be determined by the UL channel capacity not by the range capability.

For the following analysis we assume:

- Frequency: 2000 MHz
- Base Station Configuration: 3-sectors, frequency reuse of 1, Rx antennas = 2 with MU-MIMO in the UL
- Channel BW: 5.0 MHz TDD
- Path Loss Model: ITU-R 2135-1 Large City Urban
- Housing Unit Density: 4000 HU/sq-mi (1545 HU/sq-km)
- Area to be Covered: 10 sq-mi

The following table summarizes the benefits of supporting 64QAM in the UL and an UL to DL ratio biased towards the UL.

Table 13: Summary of 64 QAM benefits

	16QAM & 3/4 Coding	16QAM & 3/4 Coding	64QAM & 5/6 Coding	64QAM & 5/6 Coding
UL/DL Ratio	23/24	30/17	23/24	30/17
BS Required	64	55	60	52
BS CAPEX Impact	Reference	-14 %	-6.3 %	-19 %

Support for 64QAM with 5/6 coding in the UL plus support with TDD profiles for an UL to DL ratio up to 30/17 results in almost 20% reduction in the number of required base stations in a dense urban environment. Considering the BS site acquisition costs, civil works, and other infrastructure plus the wireless equipment, this adds up to a considerable cost savings for utility Smart Grid networks that is applicable to 11 % of the US population.

12.4 System Analysis Summary

- Proposed WiGRID System Profiles makes 802.16e a more optimal solution for Utility Smart Grid Applications in both Range-Constrained and Capacity-Constrained deployments
- WiGRID Delivers;

  Reduced CAPEX for any rollout (20 to 30%)

  Extends operational range (4x)

  Higher channel capacity for Uplink-Centric Applications (like Remote Site Monitoring)

13. Conclusions and Recommendations

The key performance requirements for a ***Wireless Smart Grid Network*** differ considerably from wireless solutions optimized for a ***Mobile Broadband Network.*** Currently available WiMAX-802.16e system profiles, optimized for the latter, have many features that make it an attractive short term solution for utilities anxious to move forward with Smart Grid deployments but lack some key essential features for an optimal long term Smart Grid network solution.

The features and system profiles proposed in this document are intended to address the added requirements for Smart Grid networks. The following table highlights key differences between Mobile Broadband and Smart Grid applications.

Table 14: Key differences between Mobile Broadband and Smart Grid

	WiMAX/802.16e for Mobile Broadband Network	WiGRID for Smart Grid Network
Frequency Bands	• Primarily licensed • Dedicated bands country by country	• No bands specifically allocated in the US • Under-utilized bands, share with other operators • Some network segments will use “lightly” licensed or license-exempt spectrum • Smaller channel BWs to facilitate spectrum sharing • Interference management will be more important
UL and DL Traffic Patterns	• DL traffic is dominant	• UL traffic is dominant • Exception will be when firmware upgrades are downloaded • Need both UL and DL bias for TDD
End-Users	• End-users will be mobile • Relatively few simultaneously active users per channel • DL files can be large	• Actors/terminals will be primarily fixed • In an AMI network there can be 1000s of simultaneous users at any given time • UL message (packet) sizes tend to be small
Mobility Requirements	• Very important	• High mobility not important • Nomadic is very important for mobile workforce
Security Requirements	• Privacy concerns	• Privacy and user-behavior patterns • Protection against malicious network attacks very important
Network Robustness	• Important	• Very important • Support for Relaying, Multi-hop, and self-configuring network (No single point-of-failure)
Latency	• Important for latency-sensitive applications: VoIP, rt Gaming, etc	• Must meet varied requirements for data payloads –3 or more sub-levels within UGS? (Low, Med, High) • Real-time UL video for disaster recovery
Coverage	• Ubiquity very desirable	• Ubiquity is essential • Extended range and Multi-hop for rural coverage • Support for M2M and/or Relay for enhanced urban coverage

In addition to the work of the WiMAX® Forum SGWG, the IEEE working groups for 802.16n [8] and 802.16p [9] are also developing features and attributes specific to Smart Grid applications. The NIST-Smart Grid Interoperability Panel (SGIP) and OpenSG Users Group are also continuing their work on defining Smart Grid network requirements. In the interest of moving forward, a 2-phase approach is proposed. The first phase takes advantage of features already defined in 802.16 and the second phase will take advantage of the IEEE 802.16n [8] and IEEE 802.16p amendments [9] with additional features applicable for Smart Grid. With the anticipated completion of the SGIP/OpenSG work at the end of 2012, the SGWG will have the opportunity to review and revise the Phase 2 features for long term Smart Grid compliance in 2013.

13.1 Recommendation

The SGWG recommends that TWG and NWG proceed immediately with system profiles based on the proposed WiGRID-1 features in this document.

The SGWG further recommends that TWG reviews and gains familiarity with the 802.16n [8] and 802.16p [9] amendments. This will help to ensure a smooth transition for WiGRID1 to WiGRID-2.

Following these recommendations will ensure that WiMAX has a timely solution specific to Smart Grid applications in the short term with WiGRID-1 and in the long term with WiGRID-2.